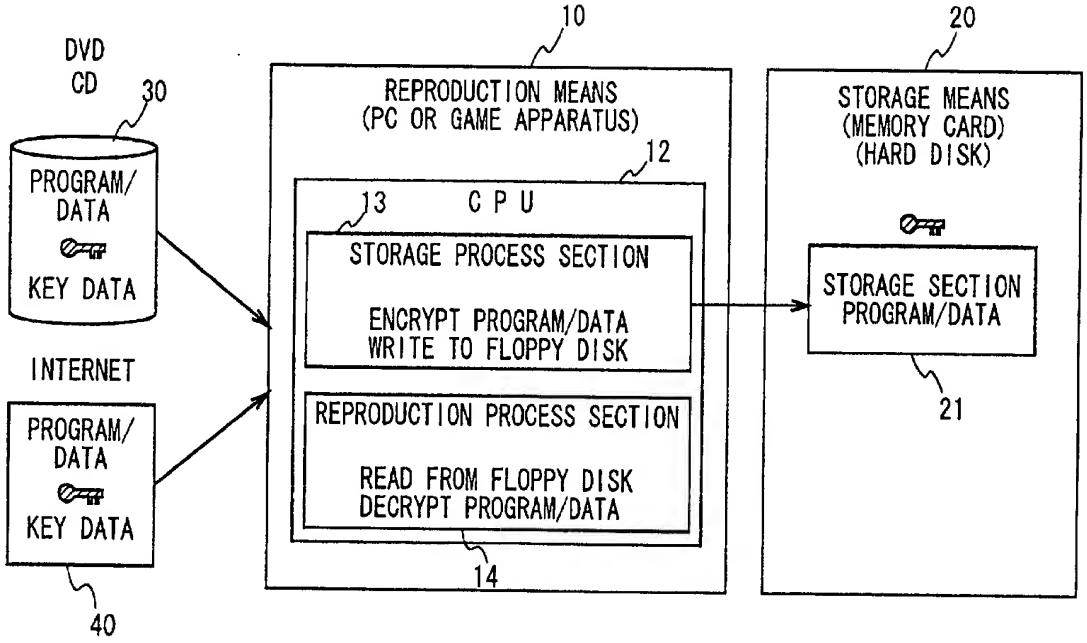


FIG. 1

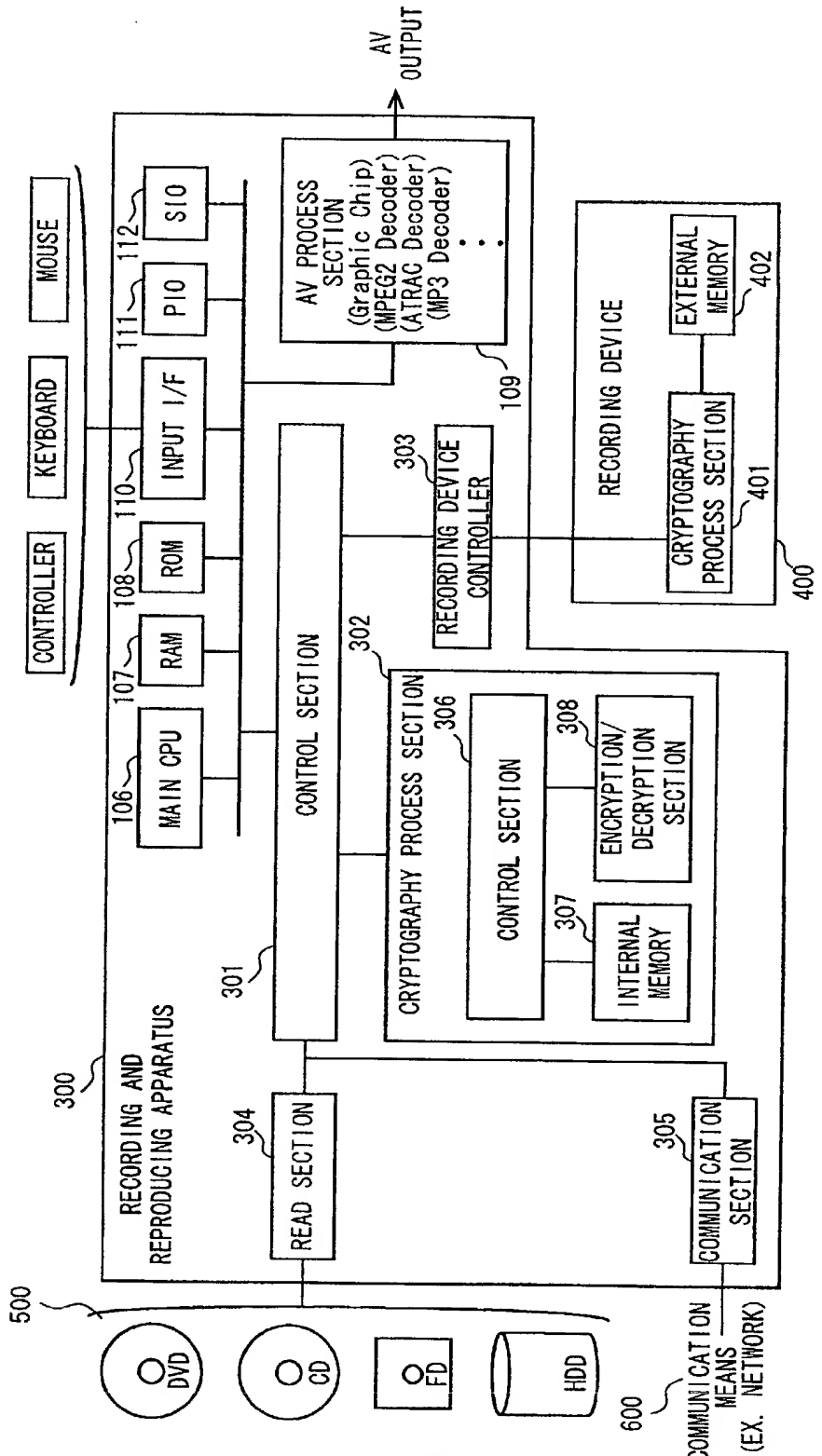

AV OUTPUT
MOUSE
KEYBOARD
CONTROLLER
SIO
PIO
INPUT I/F
ROM
RAM
MAIN CPU
AV PROCESS SECTION
(Graphic Chip)
(MPEG2 Decoder)
(ATRAC Decoder)
(MP3 Decoder)
RECORDING DEVICE
EXTERNAL MEMORY
CRYPTOGRAPHY PROCESS SECTION
RECORDING DEVICE CONTROLLER
CONTROL SECTION
CRYPTOGRAPHY PROCESS SECTION
CONTROL SECTION
ENCRYPTION/ DECRYPTION SECTION
INTERNAL MEMORY
RECORDING AND REPRODUCING APPARATUS
READ SECTION
COMMUNICATION SECTION
DVD
CD
FD
HDD
COMMUNICATION MEANS (EX. NETWORK)
500
300
301
302
303
304
305
306
307
308
106
107
108
109
110
111
112
400
401
402
600

FIG. 2

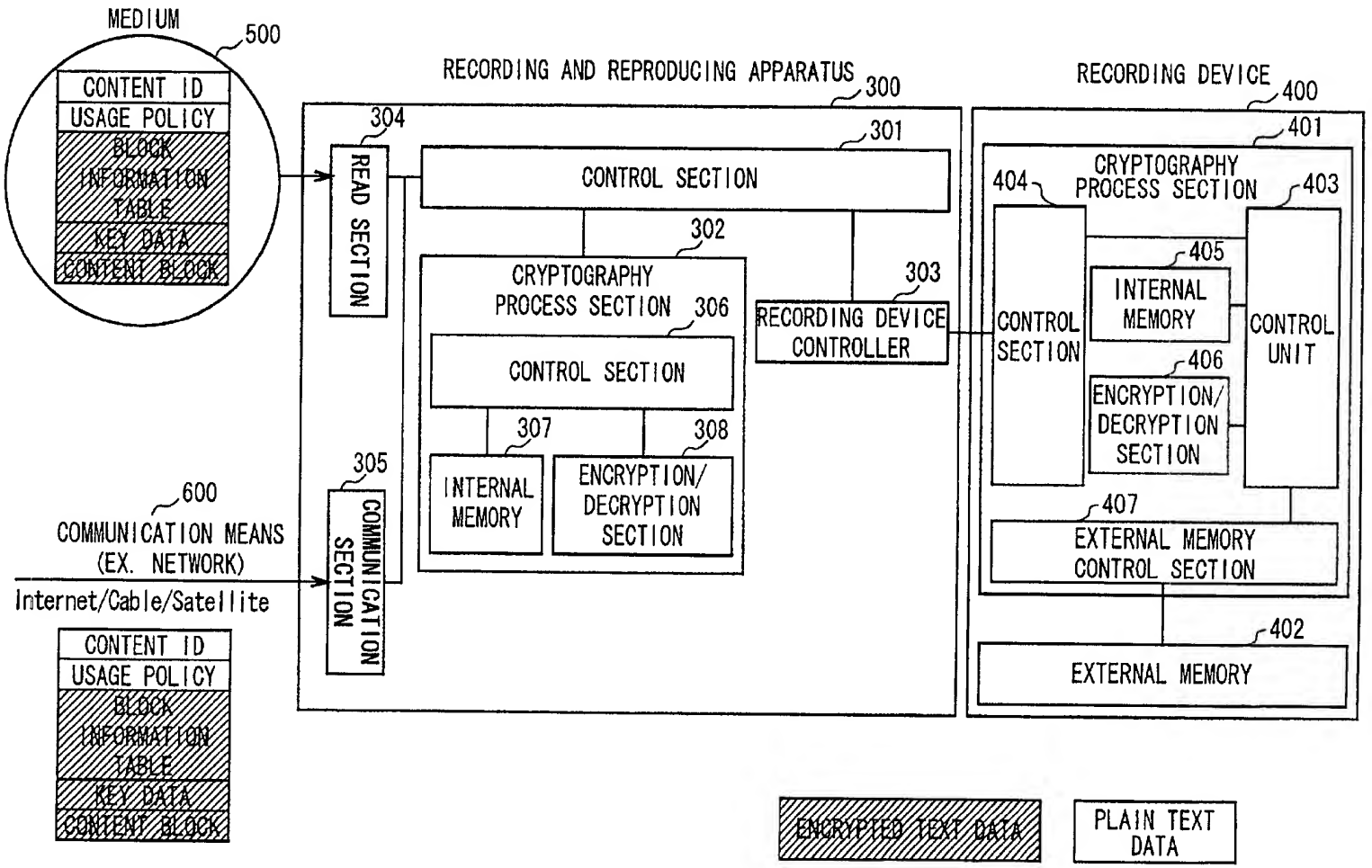
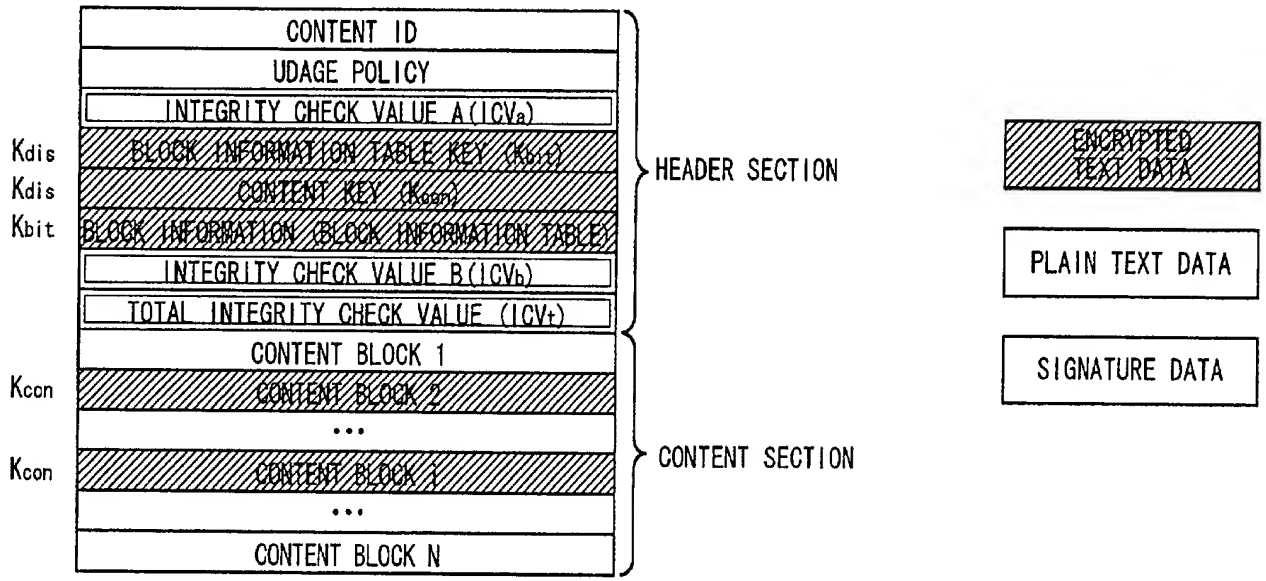


FIG. 3



DATA FORMAT ON MEDIUM AND COMMUNICATION PATH

FIG. 4

HEADER LENGTH
CONTENT LENGTH
FORMAT VERSION
FORMAT TYPE
CONTENT TYPE
OPERATION PRIORITY
LOCALIZATION FIELD
COPY PERMISSION
MOVE PERMISSION
ENCRYPTION ALGORITHM
ENCRYPTION MODE
INTEGRITY CHECK METHOD

USAGE POLICY

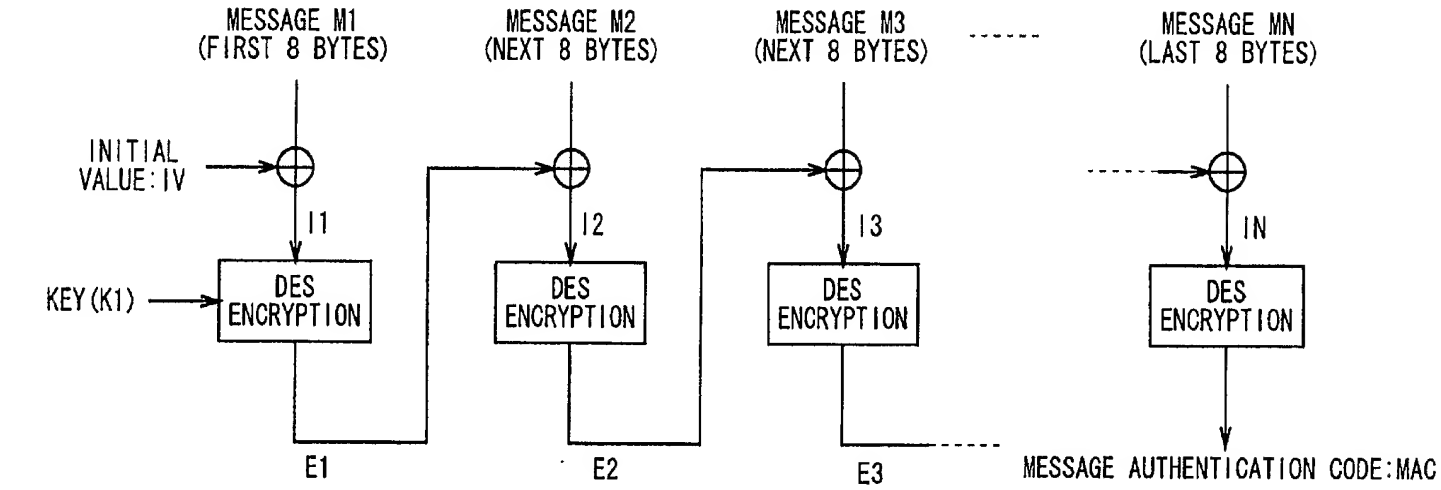
FIG. 5

Kbit

	BLOCK NUMBER
BLOCK 1	BLOCK LENGTH
	ENCRYPTION FLAG
	FLAG TO BE VERIFIED (ICV FLAG)
	ICV1
	.
	.
	.
	.
BLOCK N	BLOCK LENGTH
	ENCRYPTION FLAG
	ICV FLAG
	CONTENT INTEGRITY CHECK VALUE (ICVN)

BLOCK INFORMATION TABLE

FIG. 6



⊕:EXCLUSIVE OR (XOR) PROCESS (8-BYTE UNIT)

FIG. 7

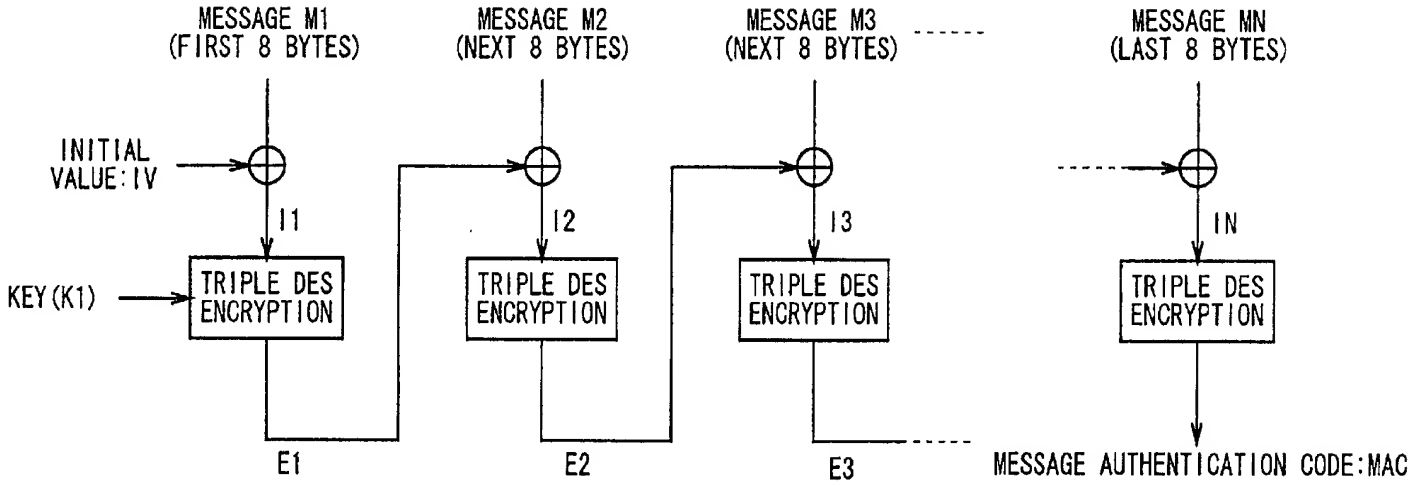

MESSAGE M1
(FIRST 8 BYTES)
MESSAGE M2
(NEXT 8 BYTES)
MESSAGE M3
(NEXT 8 BYTES)
MESSAGE MN
(LAST 8 BYTES)
INITIAL
VALUE:IV
I1
I2
I3
IN
KEY(K1)
TRIPLE DES
ENCRYPTION
TRIPLE DES
ENCRYPTION
TRIPLE DES
ENCRYPTION
TRIPLE DES
ENCRYPTION
E1
E2
E3
MESSAGE AUTHENTICATION CODE:MAC

FIG. 8

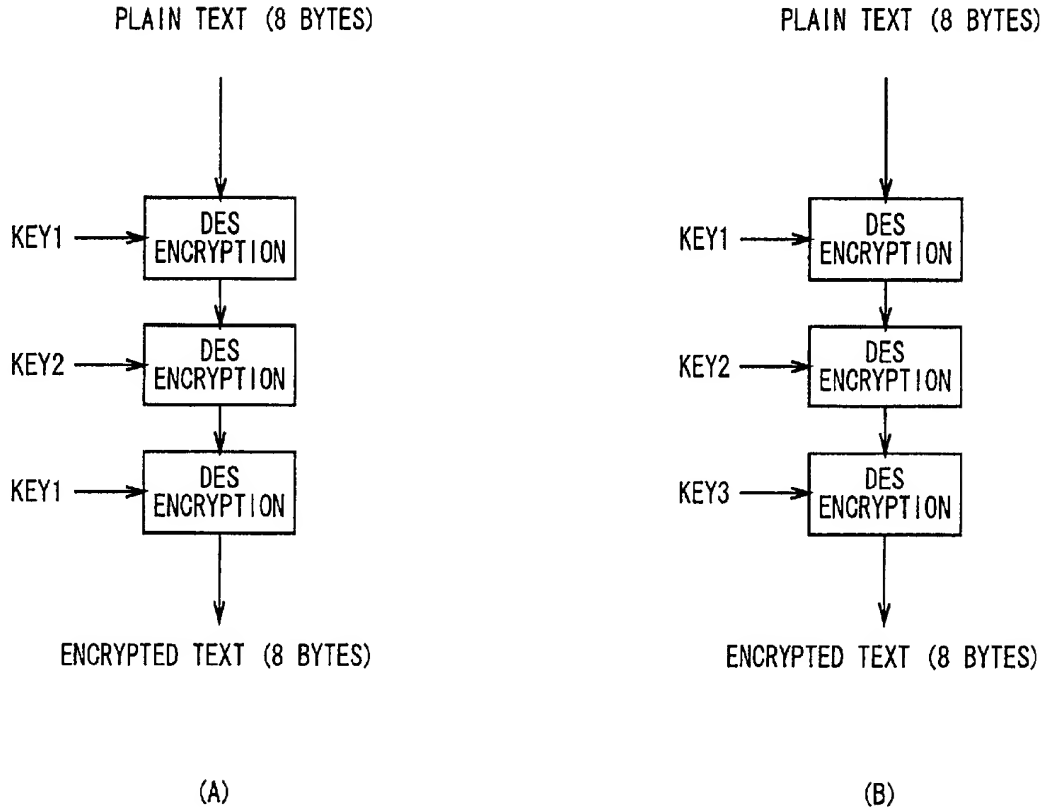


FIG. 9

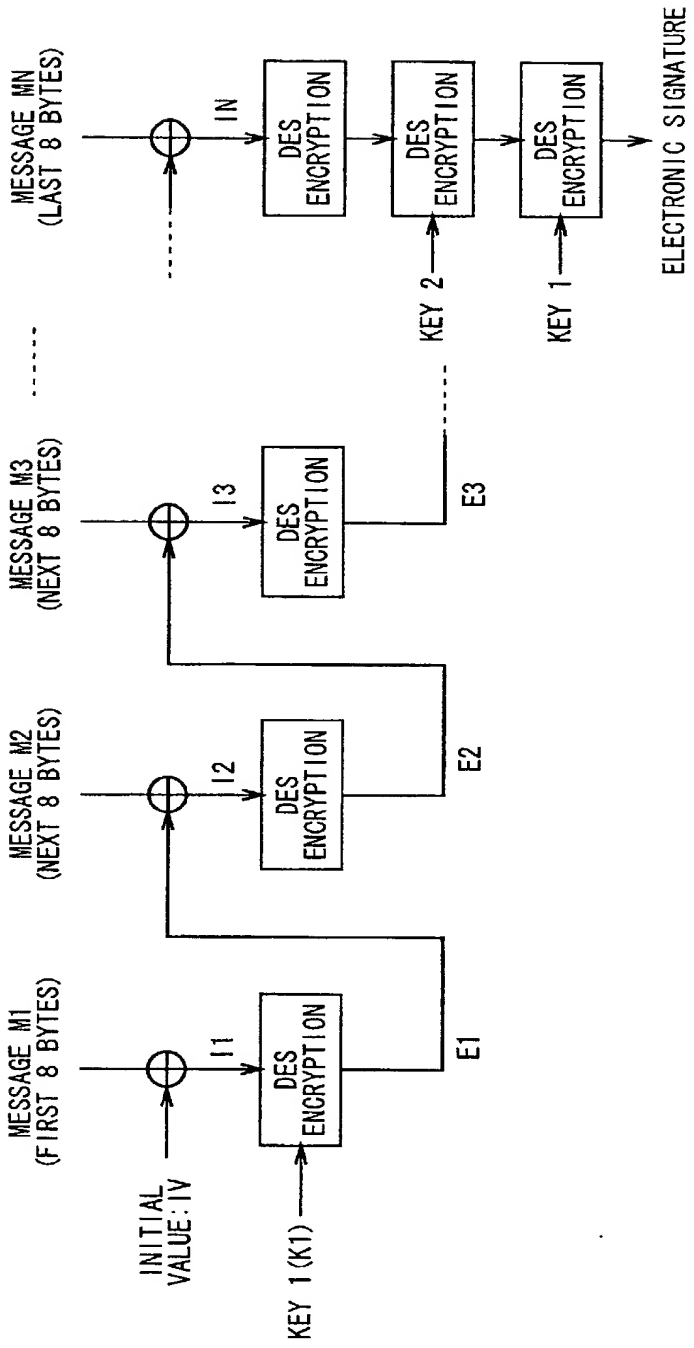
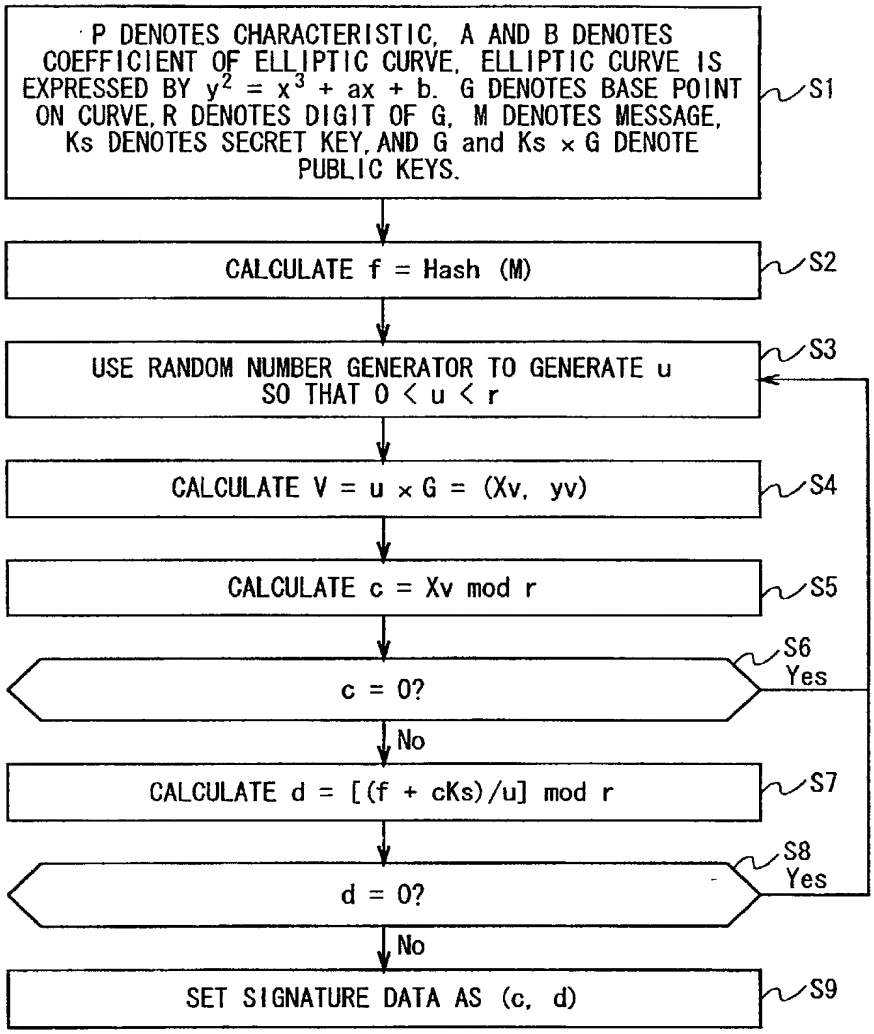

MESSAGE M1
(FIRST 8 BYTES)
MESSAGE M2
(NEXT 8 BYTES)
MESSAGE M3
(NEXT 8 BYTES)
MESSAGE MN
(LAST 8 BYTES)
INITIAL
VALUE:IV
KEY 1 (K1)
I1
I2
I3
IN
DES
ENCRYPTION
E1
E2
E3
KEY 2
KEY 1
ELECTRONIC SIGNATURE

FIG. 10

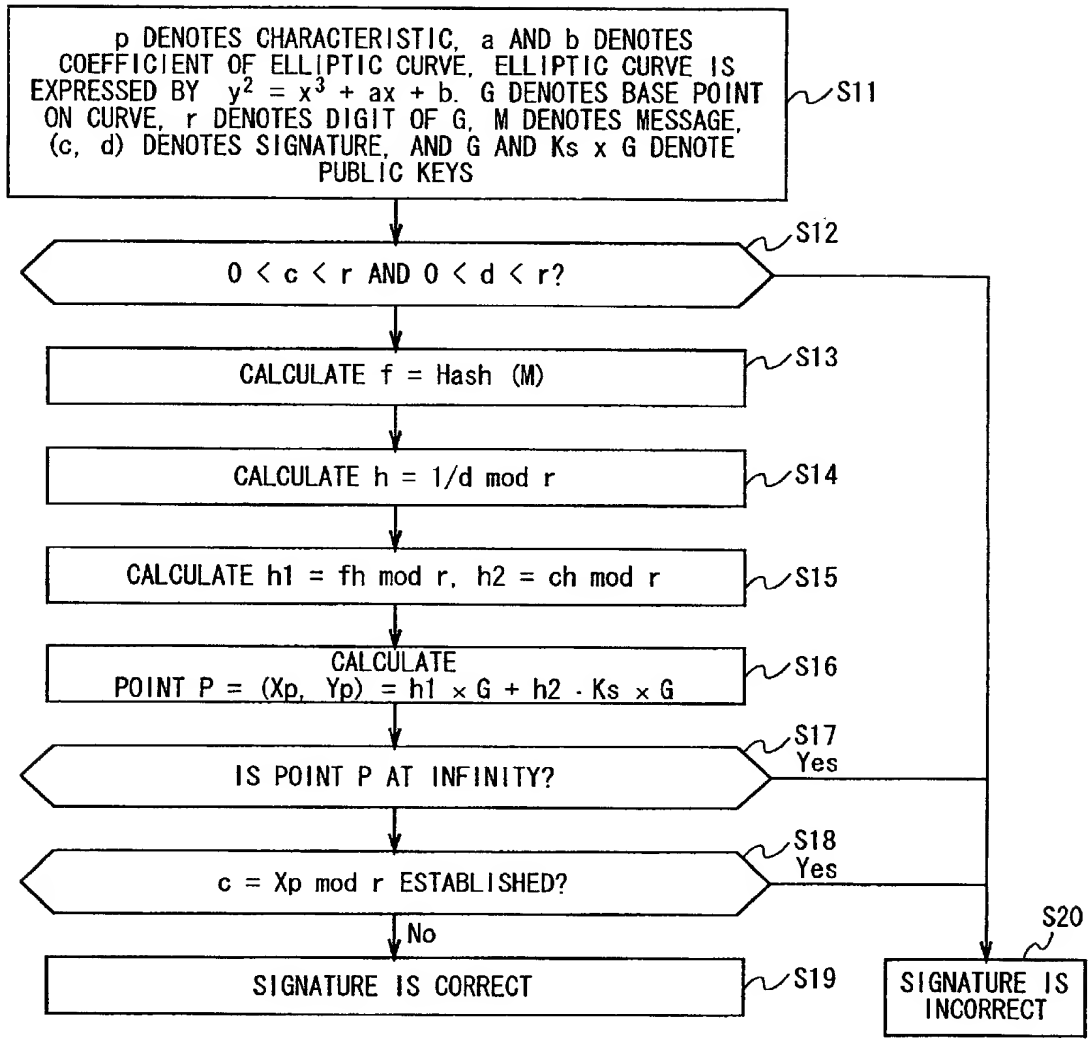
SIGNATURE GENERATION



GENERATION OF SIGNATURE (IEEE P1363/D3)

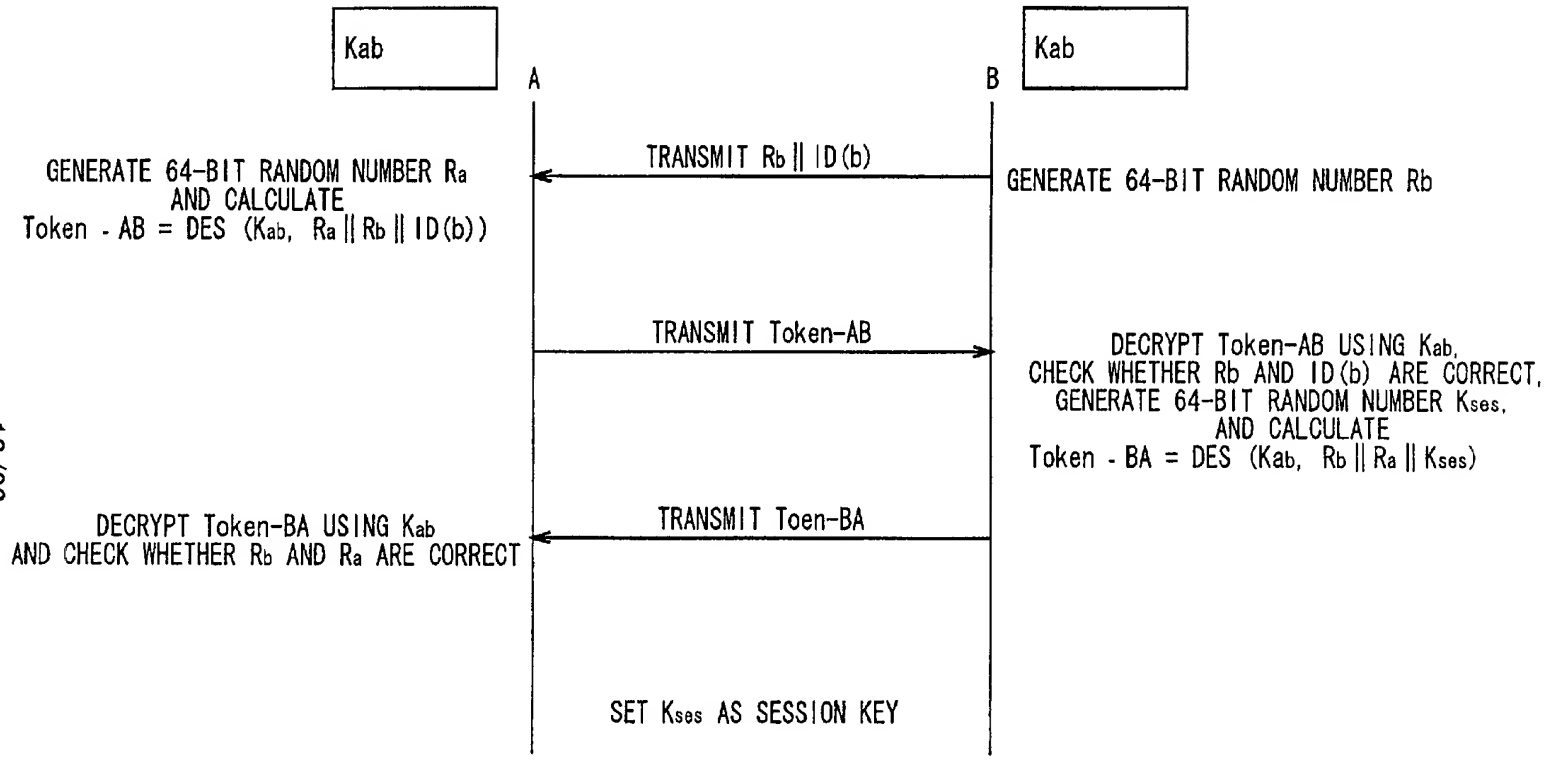
FIG. 11

SIGNATURE VERIFICATION



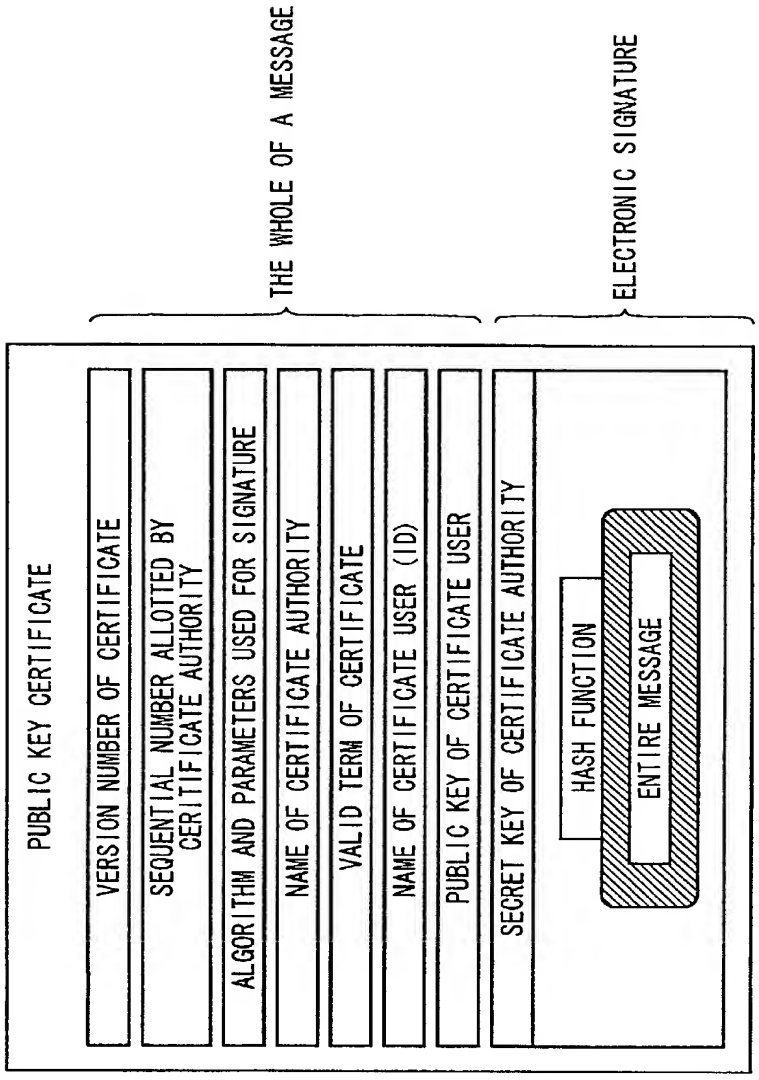
SIGNATURE VERIFICATION(IEEE P1363/D3)

FIG. 12



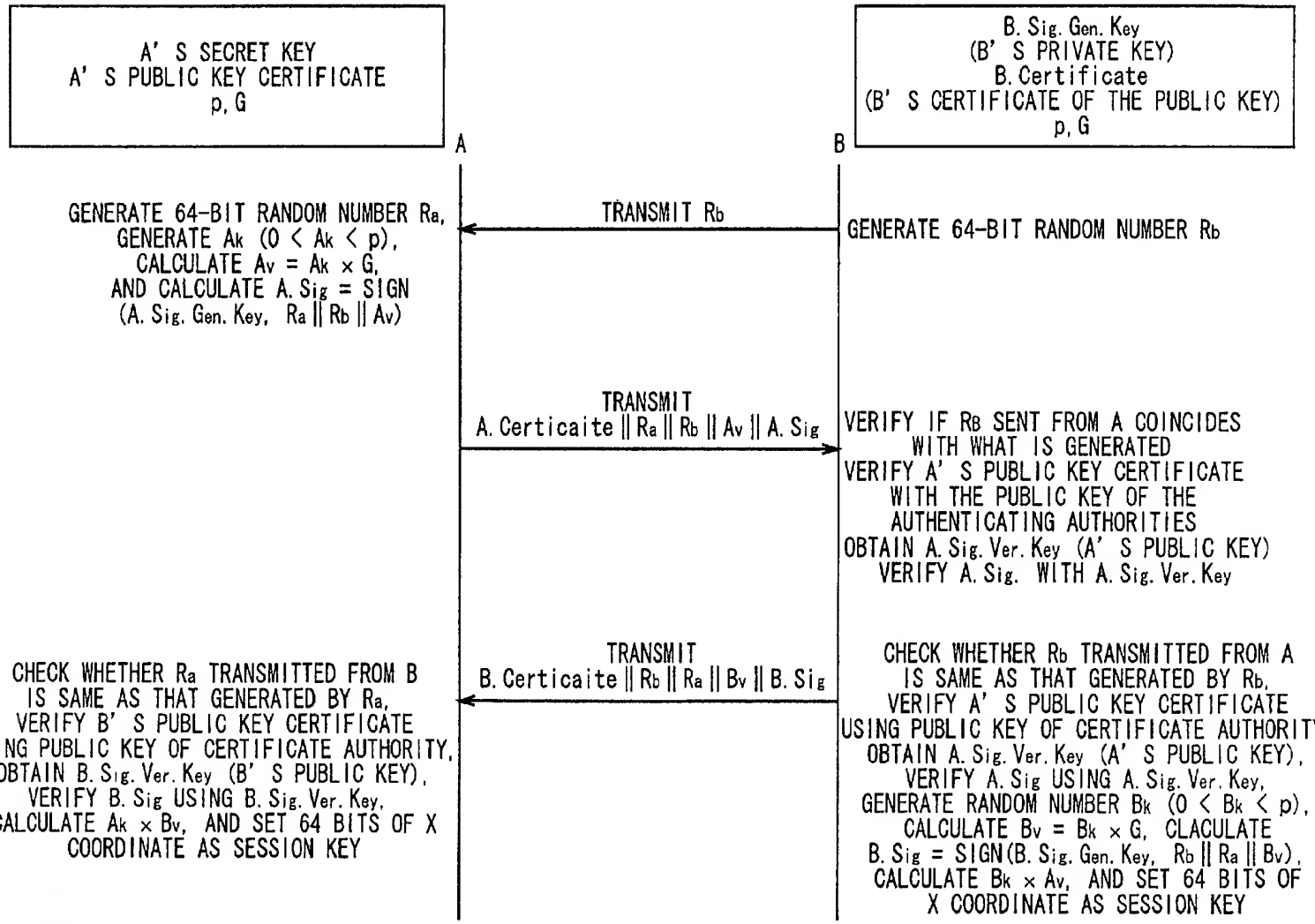
ISO/IEC 9798-2 MUTUAL AUTHENTICATION AND KEY SHARING METHOD USING SYMMETRICAL KEY CRYPTOGRAPHY TECHNIQUE

FIG. 13



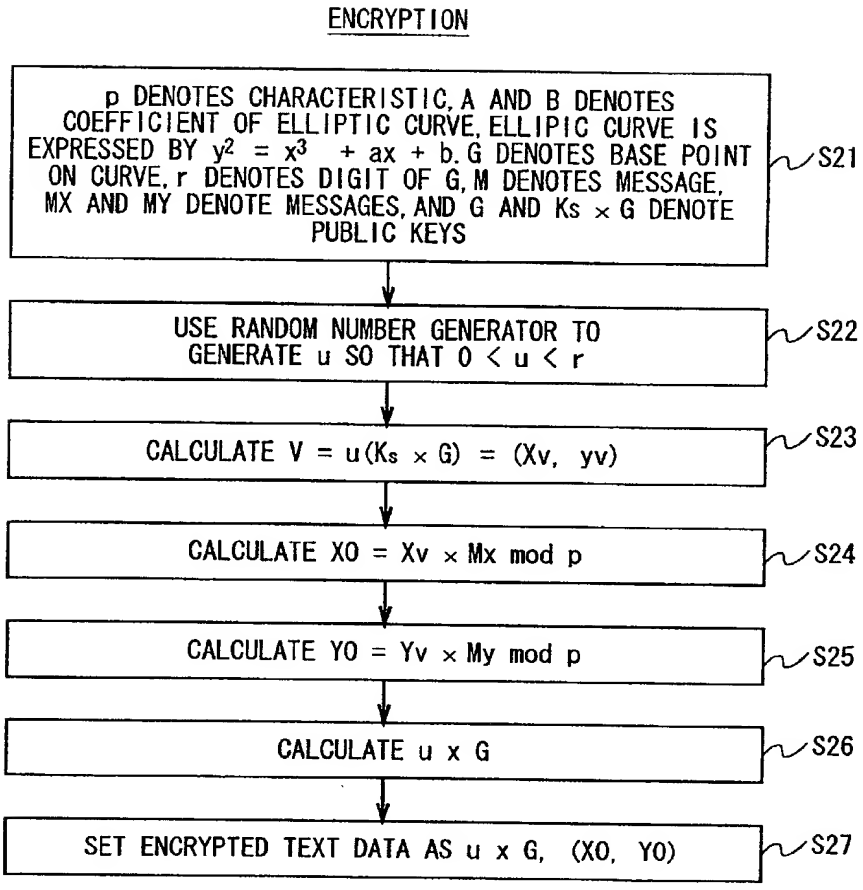
PUBLIC KEY CERTIFICATE

FIG. 14



ISO/IEC 9798-3 MUTUAL AUTHENTICATION AND KEY SHARING METHOD USING SYMMETRICAL KEY CRYPTOGRAPHY TECHNIQUE

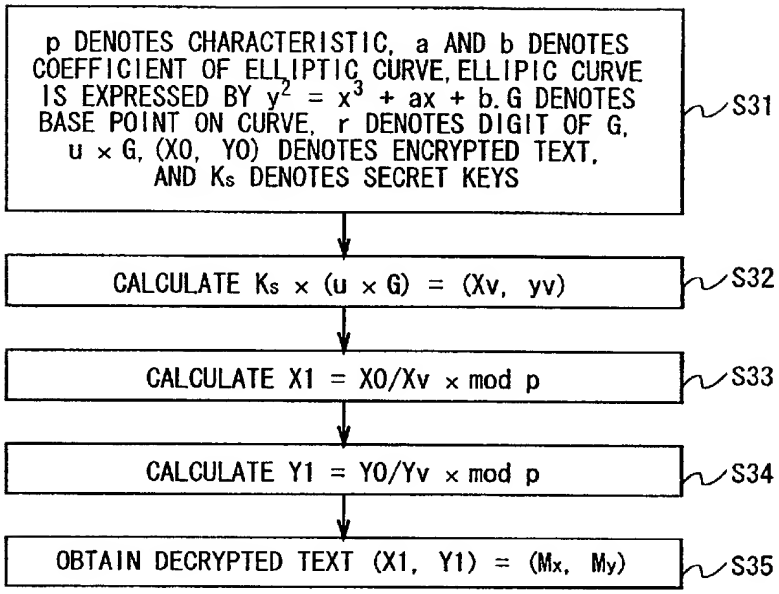
FIG. 15



ENCRYPTION USING ELLIPTIC CURVE CRYPTOGRAPHY (MENEZES-VANSTONE)

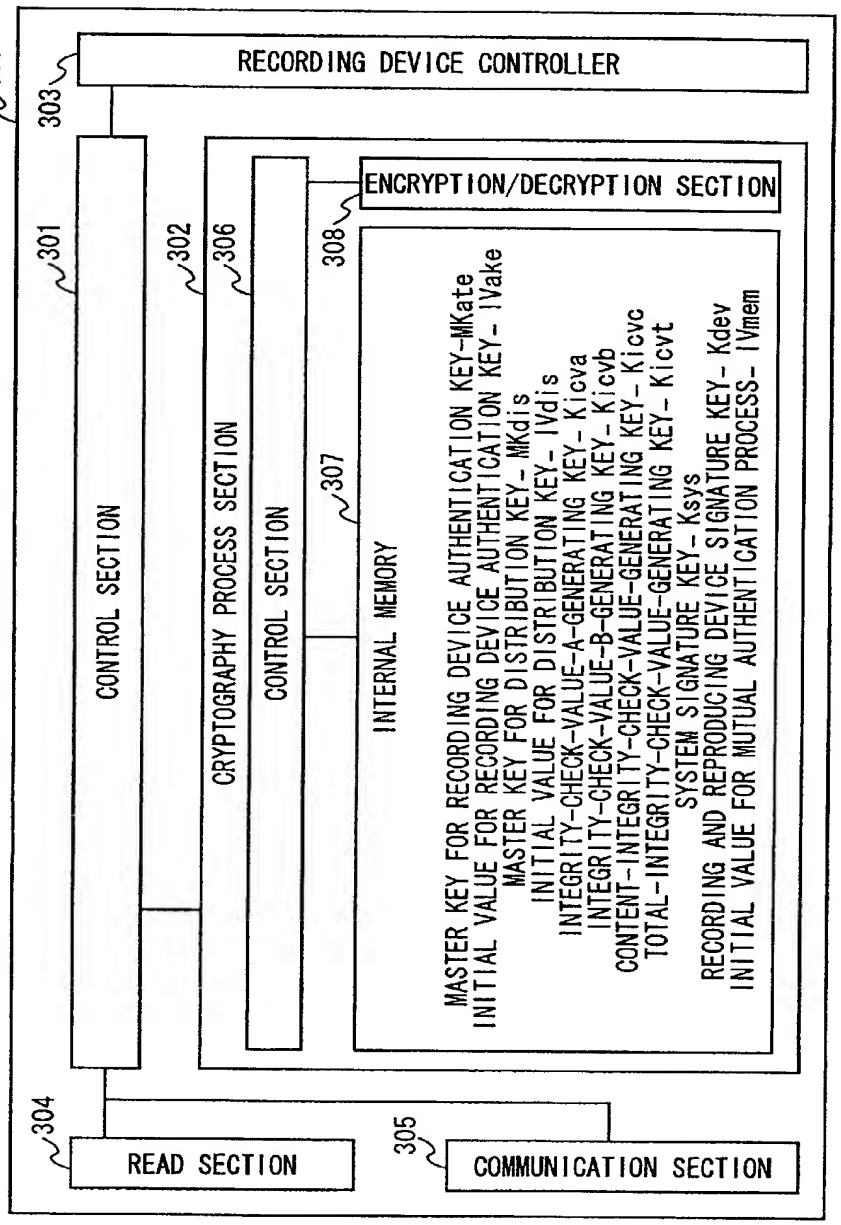
FIG. 16

DECRYPTION



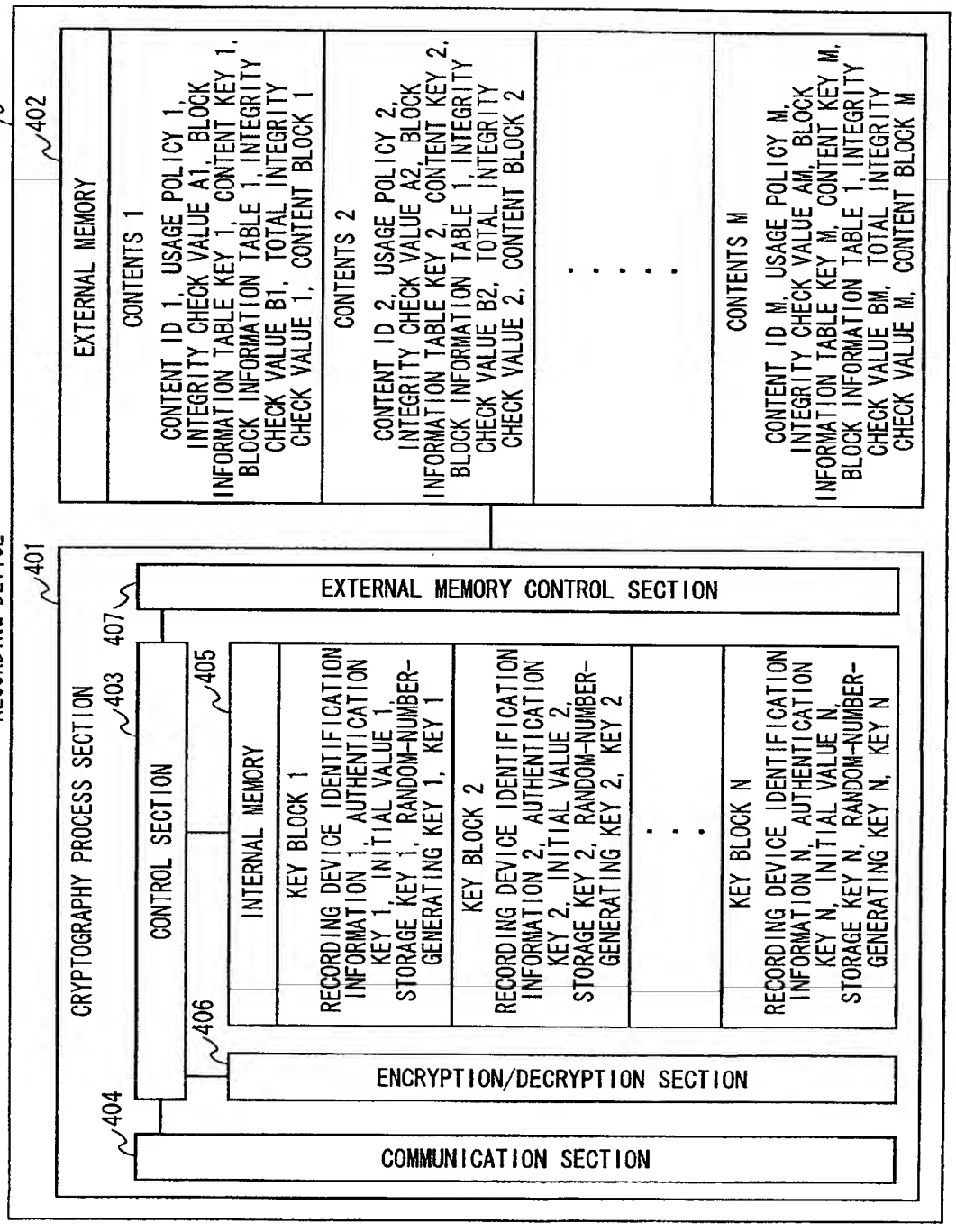
DECRYPTION USING ELLIPTIC CURVE CRYPTOGRAPHY (MENEZES-VANSTONE)

FIG. 17



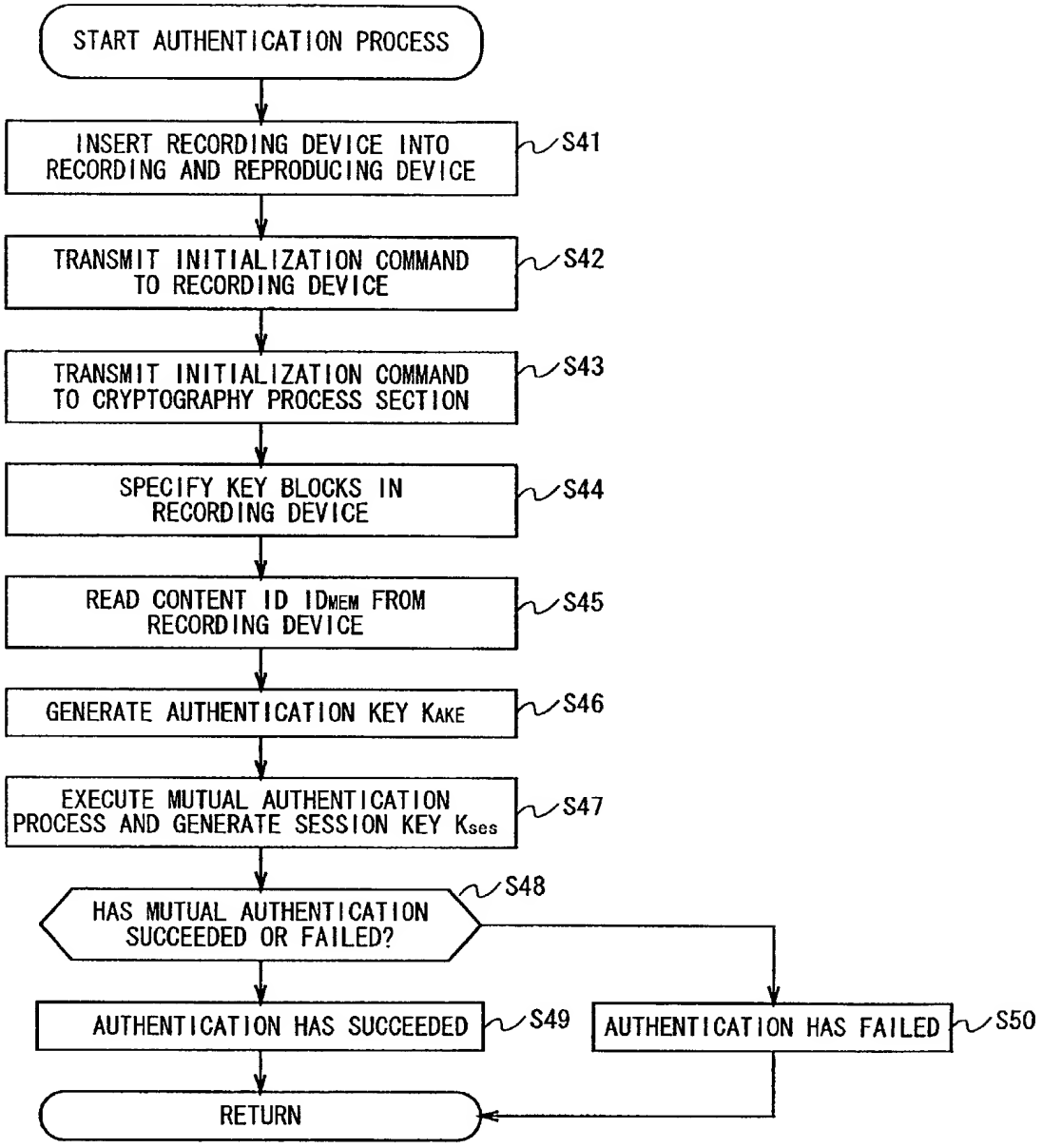
HOW DATA ARE HELD ON RECORDING AND REPRODUCING DEVICE

FIG. 18



HOW DATA ARE HELD ON RECORDING DEVICE

FIG. 19



MUTUAL AUTHENTICATION BETWEEN RECORDING AND REPRODUCING DEVICE AND RECORDING DEVICE

FIG. 20

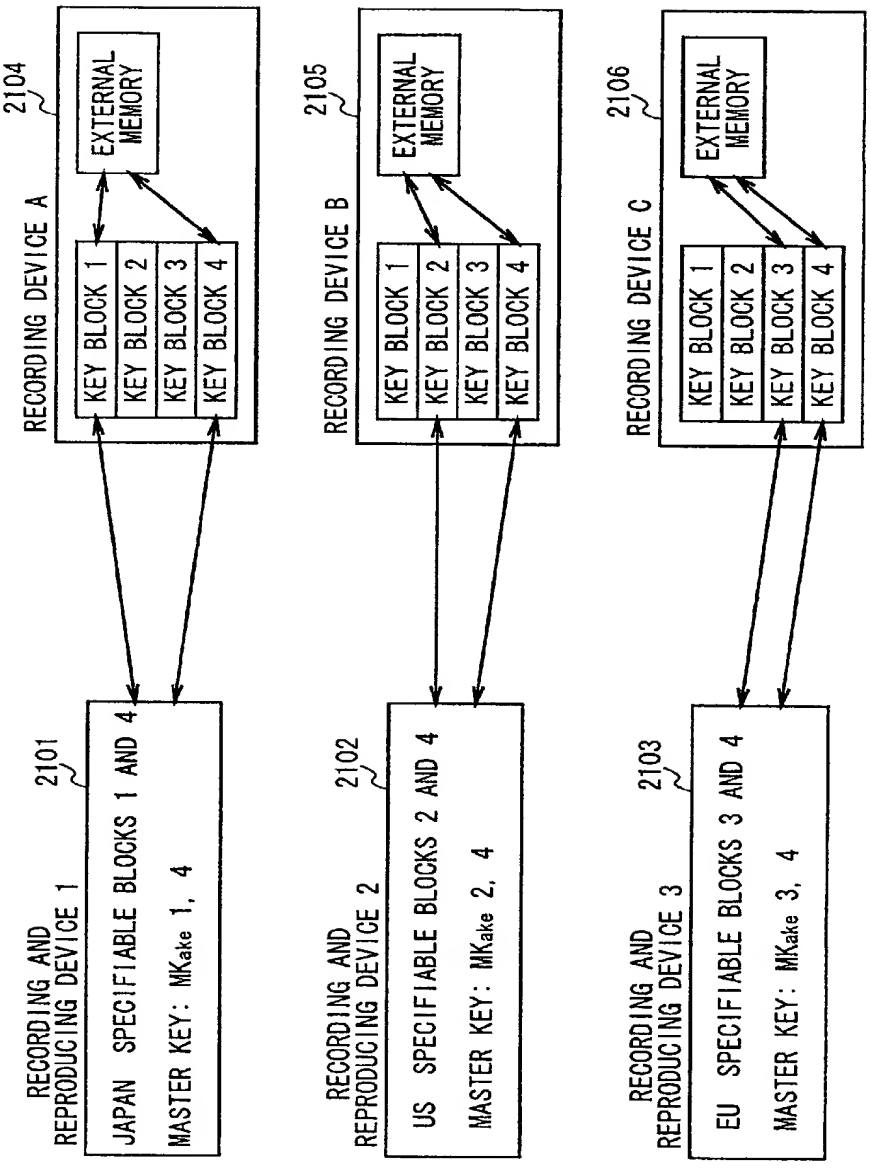
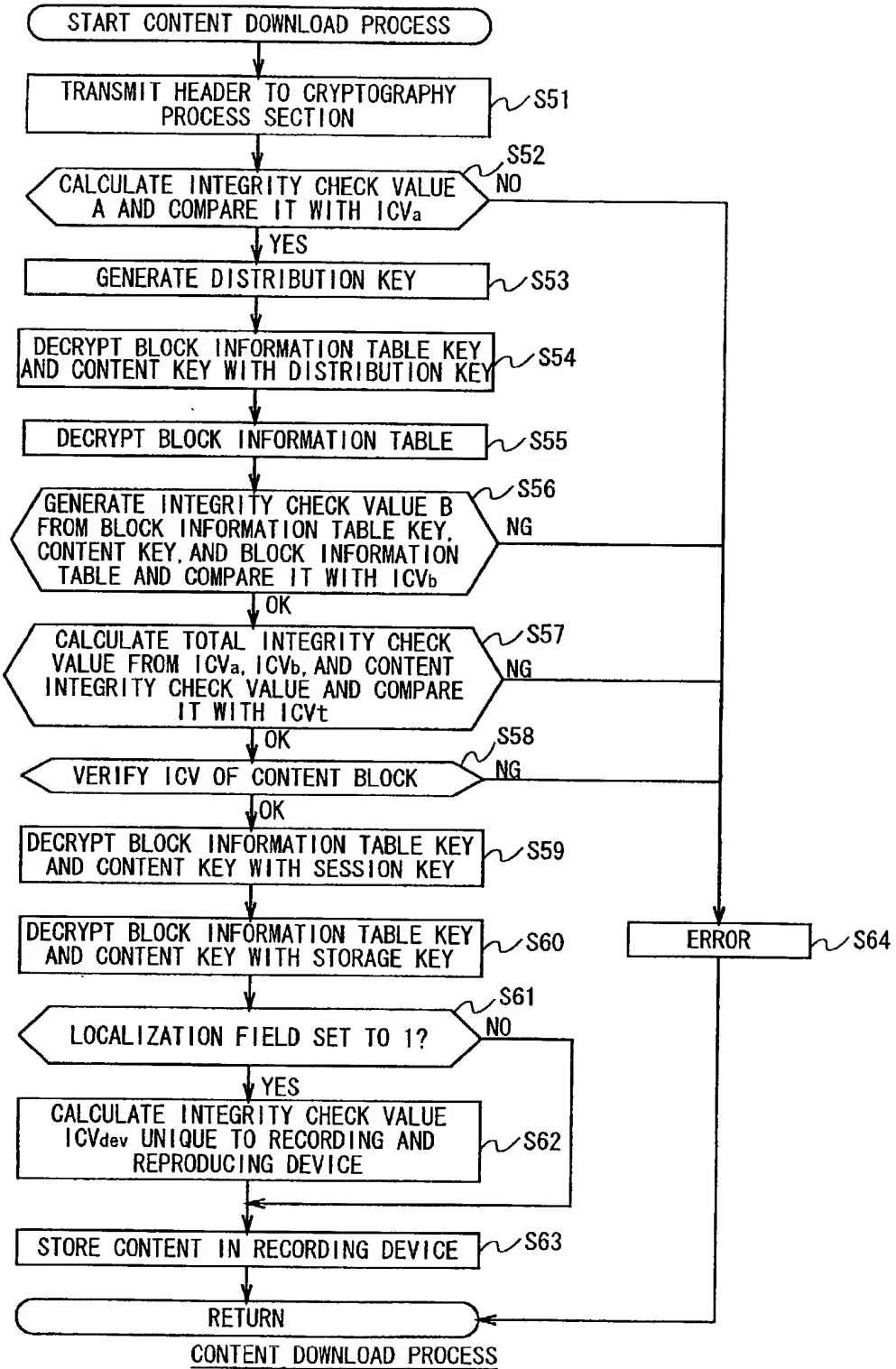
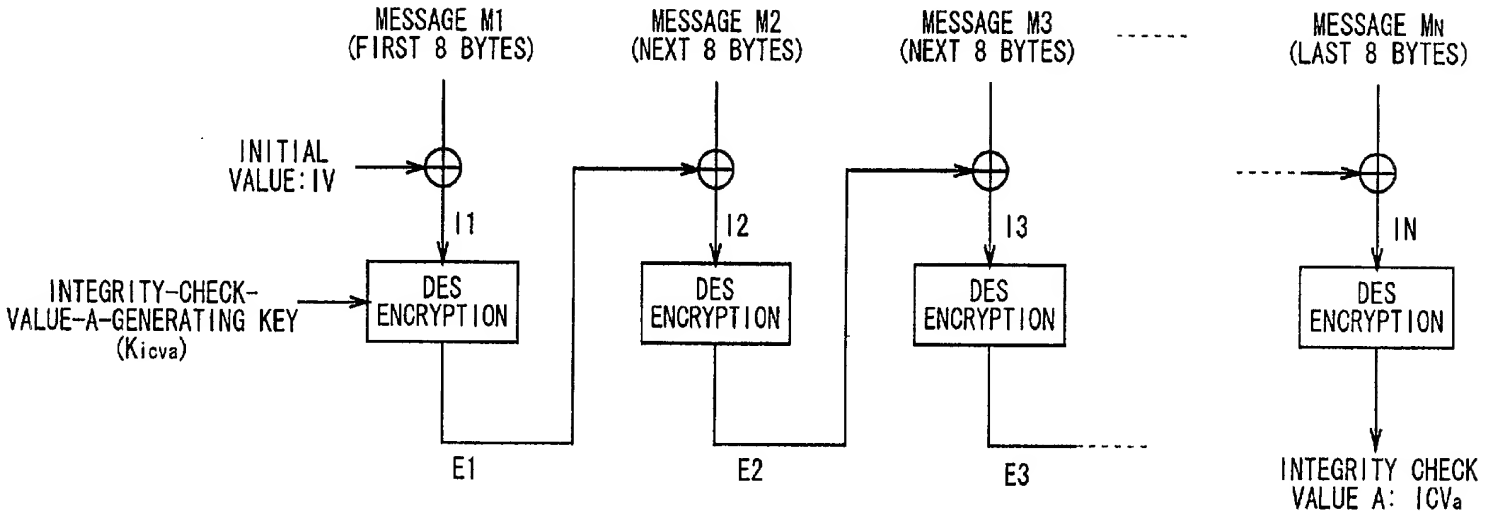

RECORDING AND REPRODUCING DEVICE 1
2101
JAPAN SPECIFIABLE BLOCKS 1 AND 4
MASTER KEY: MKake 1, 4
RECORDING AND REPRODUCING DEVICE 2
2102
US SPECIFIABLE BLOCKS 2 AND 4
MASTER KEY: MKake 2, 4
RECORDING AND REPRODUCING DEVICE 3
2103
EU SPECIFIABLE BLOCKS 3 AND 4
MASTER KEY: MKake 3, 4
RECORDING DEVICE A
2104
KEY BLOCK 1
KEY BLOCK 2
KEY BLOCK 3
KEY BLOCK 4
EXTERNAL MEMORY
RECORDING DEVICE B
2105
KEY BLOCK 1
KEY BLOCK 2
KEY BLOCK 3
KEY BLOCK 4
EXTERNAL MEMORY
RECORDING DEVICE C
2106
KEY BLOCK 1
KEY BLOCK 2
KEY BLOCK 3
KEY BLOCK 4
EXTERNAL MEMORY

FIG. 21



CONTENT DOWNLOAD PROCESS

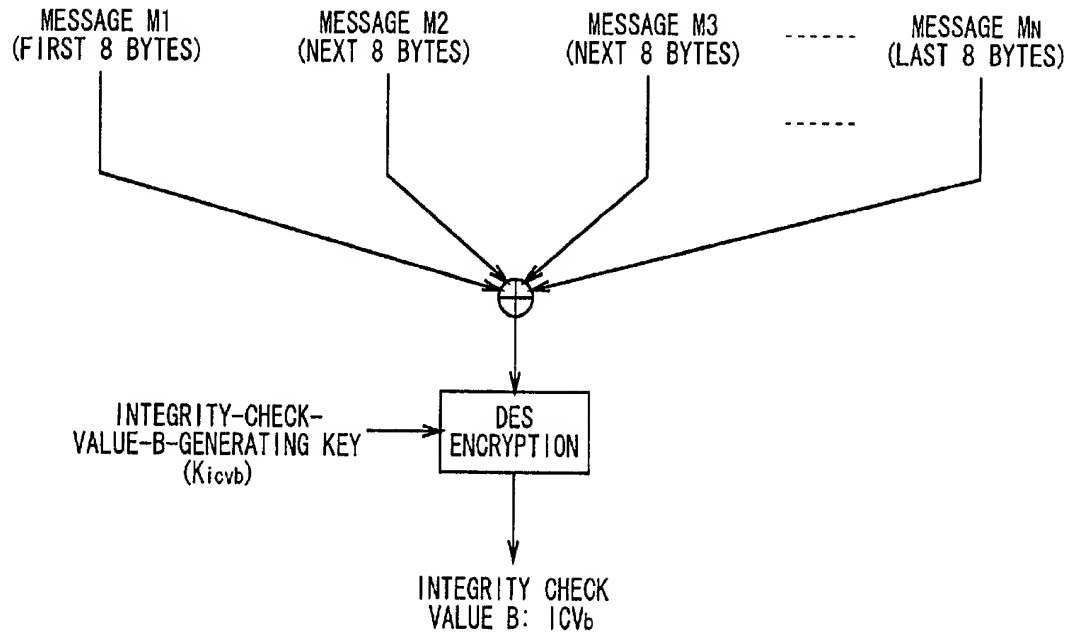
FIG. 22



MESSAGES M1 TO MN: CONTENT ID AND USAGE POLICY

⊕:EXCLUSIVE OR PROCESS (EVERY 8 BYTES)

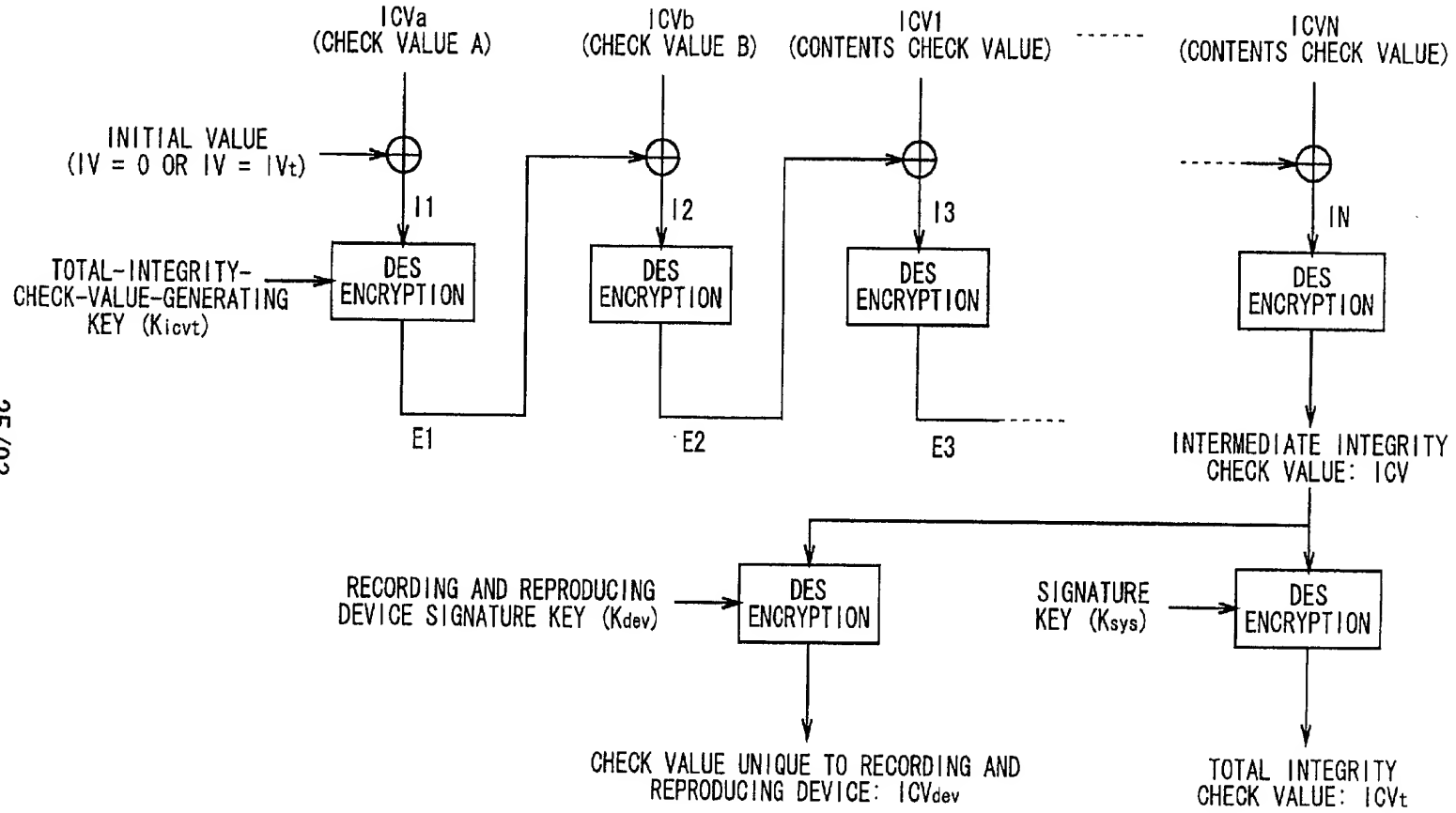
FIG. 23



MESSAGES M1 TO MN: BLOCK INFORMATION TABLE KEY K_{bit}, CONTENT KEY K_{con}, AND BLOCK INFORMATION TABLE

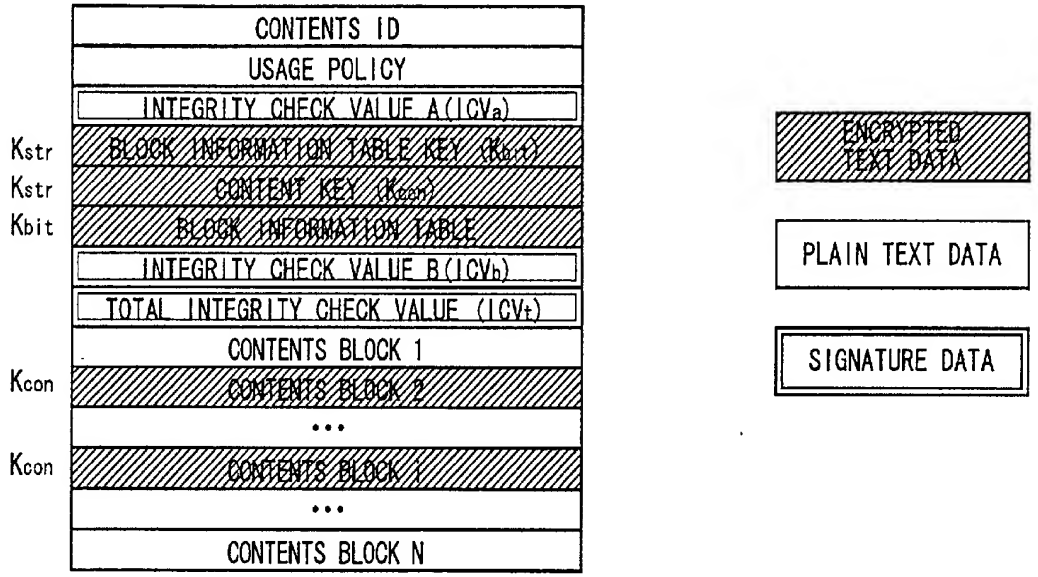
⊕:EXCLUSIVE OR PROCESS (EVERY 8 BYTES)

FIG. 24



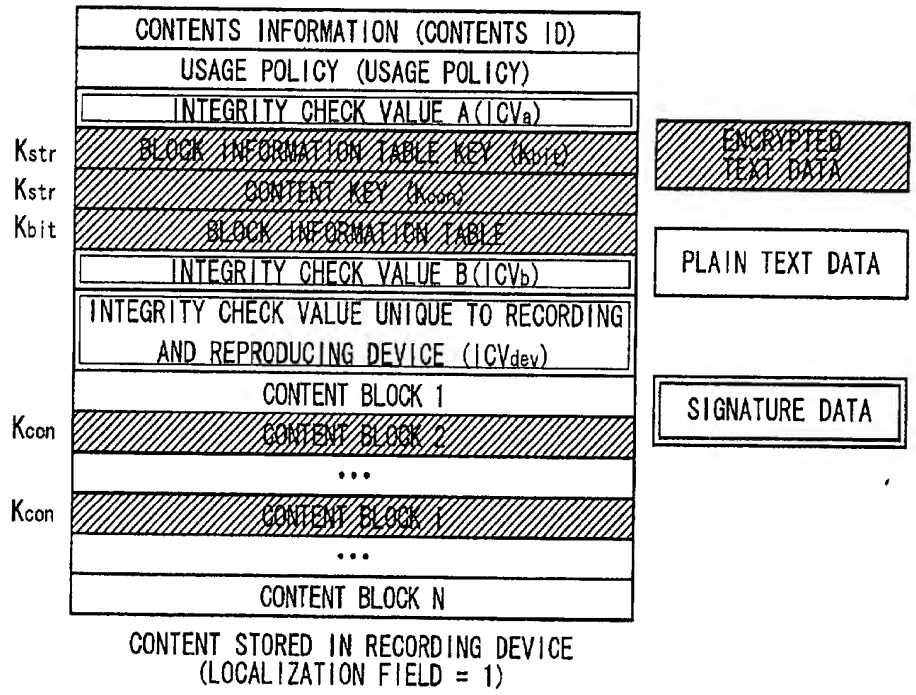
⊕:EXCLUSIVE OR PROCESS (EVERY 8 BYTES)

FIG. 25



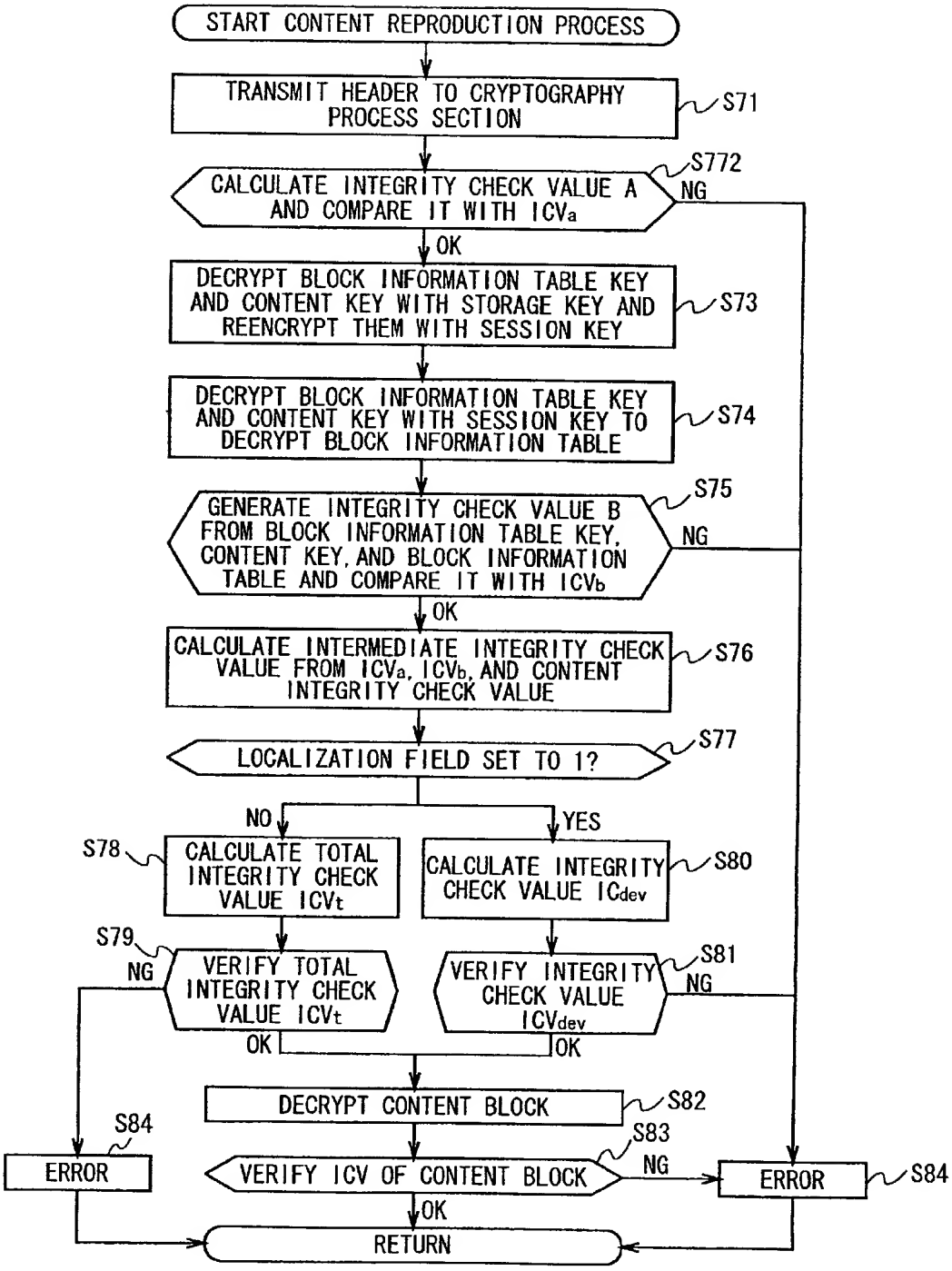
CONTENT STORED IN RECORDING DEVICE
(LOCALIZATION FIELD = 0)

FIG. 26



CONTENT STORED IN RECORDING DEVICE
(LOCALIZATION FIELD = 1)

FIG. 27



CONTENT REPRODUCTION PROCESS

FIG. 28

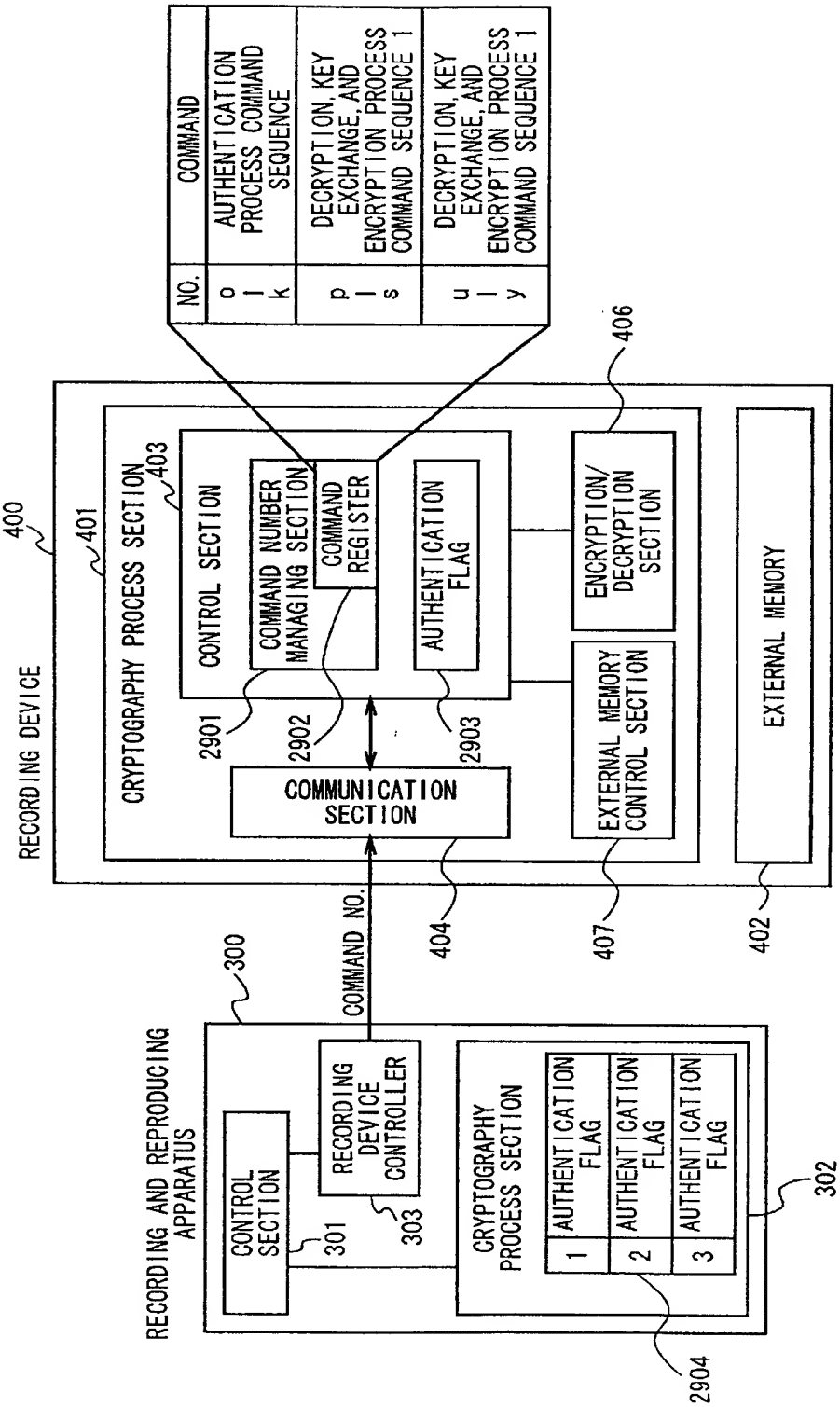

RECORDING AND REPRODUCING APPARATUS
300
CONTROL SECTION
301
RECORDING DEVICE CONTROLLER
303
CRYPTOGRAPHY PROCESS SECTION
1
AUTHENTICATION FLAG
2
AUTHENTICATION FLAG
3
AUTHENTICATION FLAG
302
2904
COMMAND NO.
RECORDING DEVICE
400
CRYPTOGRAPHY PROCESS SECTION
401
403
CONTROL SECTION
COMMAND NUMBER MANAGING SECTION
COMMAND REGISTER
AUTHENTICATION FLAG
2901
2902
2903
COMMUNICATION SECTION
404
406
ENCRYPTION/ DECRYPTION SECTION
EXTERNAL MEMORY CONTROL SECTION
407
EXTERNAL MEMORY
402
NO.
COMMAND
o
AUTHENTICATION PROCESS COMMAND SEQUENCE
p
DECRYPTION, KEY EXCHANGE, AND ENCRYPTION PROCESS COMMAND SEQUENCE 1
u
DECRYPTION, KEY EXCHANGE, AND ENCRYPTION PROCESS COMMAND SEQUENCE 1

FIG. 29

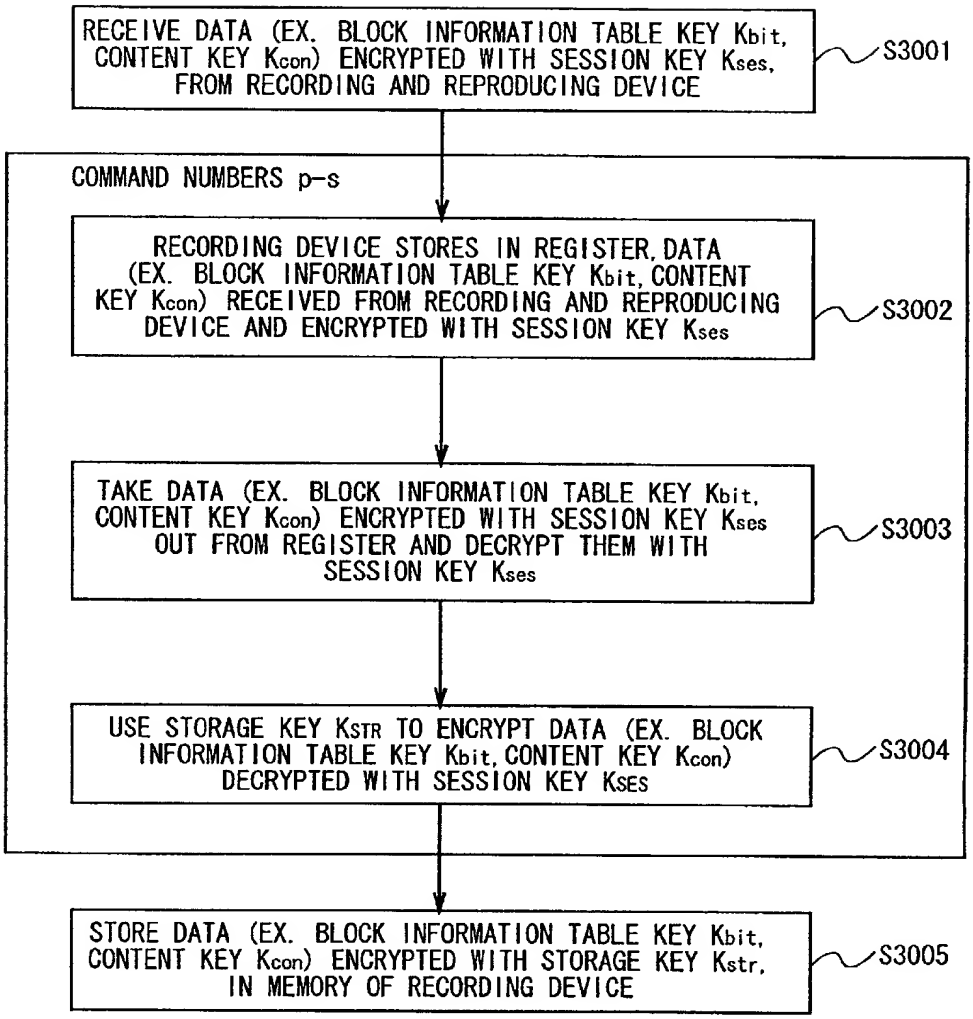

RECEIVE DATA (EX. BLOCK INFORMATION TABLE KEY Kbit, CONTENT KEY Kcon) ENCRYPTED WITH SESSION KEY Kses, FROM RECORDING AND REPRODUCING DEVICE
S3001
COMMAND NUMBERS p-s
RECORDING DEVICE STORES IN REGISTER, DATA (EX. BLOCK INFORMATION TABLE KEY Kbit, CONTENT KEY Kcon) RECEIVED FROM RECORDING AND REPRODUCING DEVICE AND ENCRYPTED WITH SESSION KEY Kses
S3002
TAKE DATA (EX. BLOCK INFORMATION TABLE KEY Kbit, CONTENT KEY Kcon) ENCRYPTED WITH SESSION KEY Kses OUT FROM REGISTER AND DECRYPT THEM WITH SESSION KEY Kses
S3003
USE STORAGE KEY KSTR TO ENCRYPT DATA (EX. BLOCK INFORMATION TABLE KEY Kbit, CONTENT KEY Kcon) DECRYPTED WITH SESSION KEY KSES
S3004
STORE DATA (EX. BLOCK INFORMATION TABLE KEY Kbit, CONTENT KEY Kcon) ENCRYPTED WITH STORAGE KEY Kstr, IN MEMORY OF RECORDING DEVICE
S3005

FIG. 30

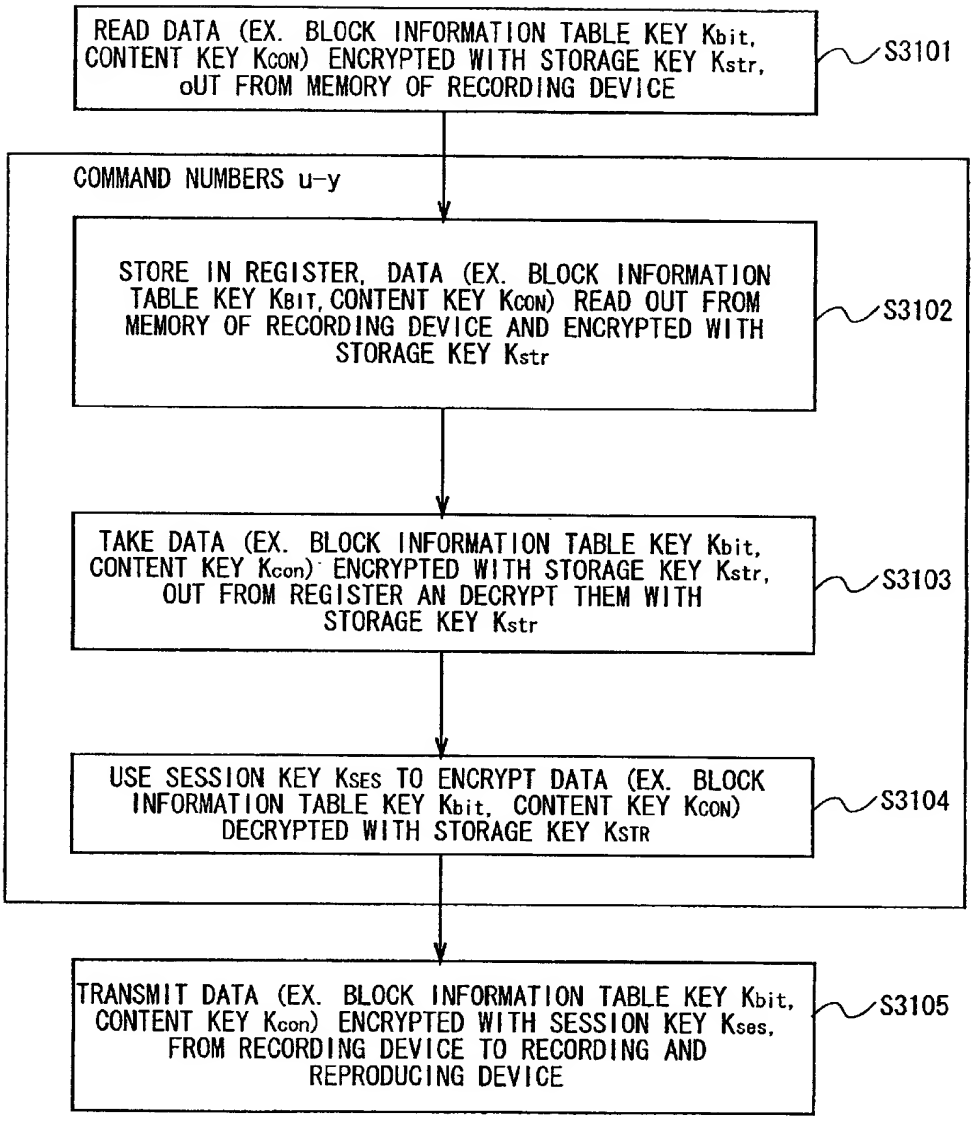

READ DATA (EX. BLOCK INFORMATION TABLE KEY Kbit, CONTENT KEY KCON) ENCRYPTED WITH STORAGE KEY Kstr, oUT FROM MEMORY OF RECORDING DEVICE
S3101
COMMAND NUMBERS u-y
STORE IN REGISTER, DATA (EX. BLOCK INFORMATION TABLE KEY KBIT, CONTENT KEY KCON) READ OUT FROM MEMORY OF RECORDING DEVICE AND ENCRYPTED WITH STORAGE KEY Kstr
S3102
TAKE DATA (EX. BLOCK INFORMATION TABLE KEY Kbit, CONTENT KEY Kcon) ENCRYPTED WITH STORAGE KEY Kstr, OUT FROM REGISTER AN DECRYPT THEM WITH STORAGE KEY Kstr
S3103
USE SESSION KEY KSES TO ENCRYPT DATA (EX. BLOCK INFORMATION TABLE KEY Kbit, CONTENT KEY KCON) DECRYPTED WITH STORAGE KEY KSTR
S3104
TRANSMIT DATA (EX. BLOCK INFORMATION TABLE KEY Kbit, CONTENT KEY Kcon) ENCRYPTED WITH SESSION KEY Kses, FROM RECORDING DEVICE TO RECORDING AND REPRODUCING DEVICE
S3105

FIG. 31

FORMAT TYPE 0

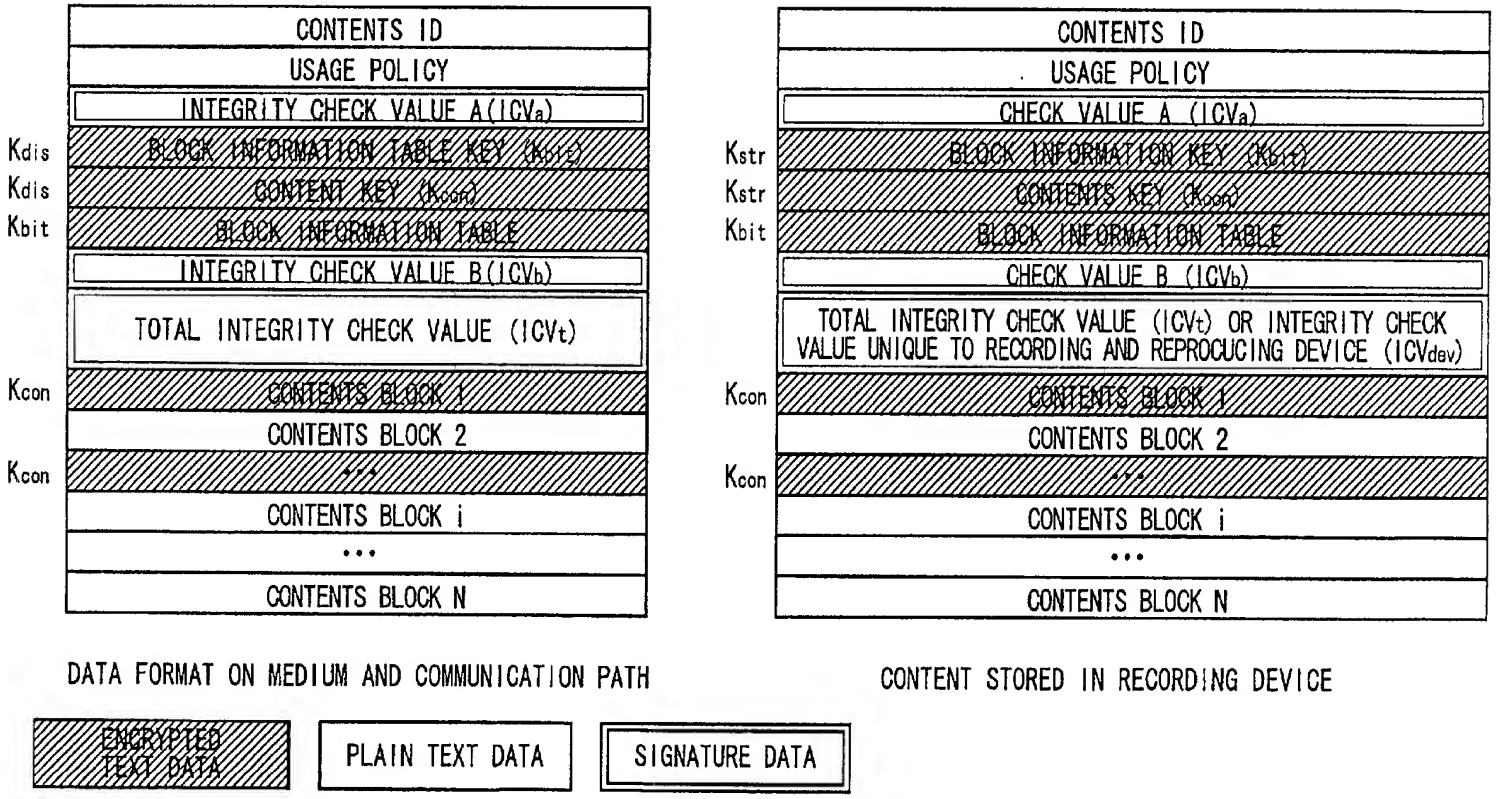


FIG. 32

FORMAT TYPE 1

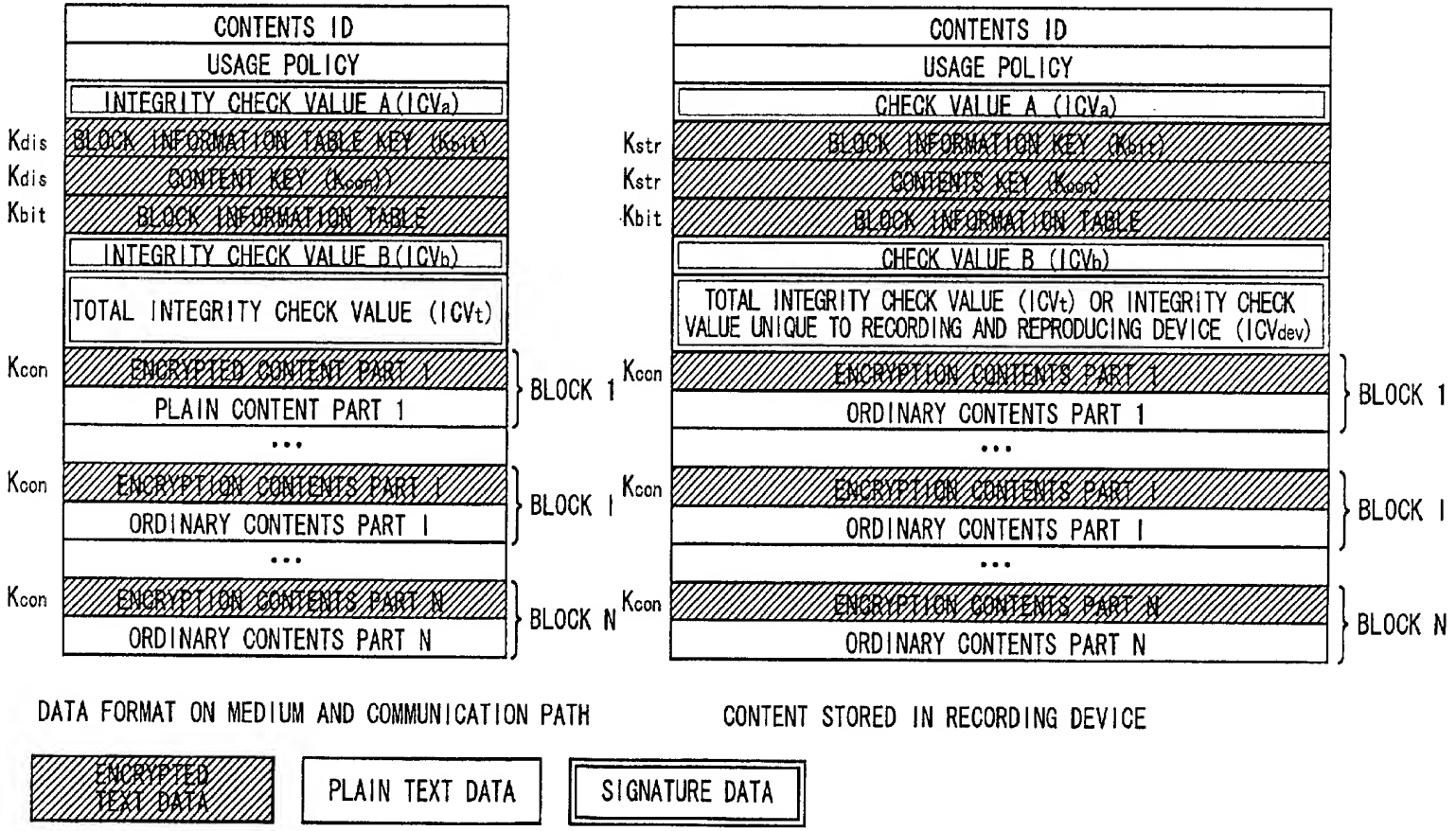


FIG. 33

FORMAT TYPE 2

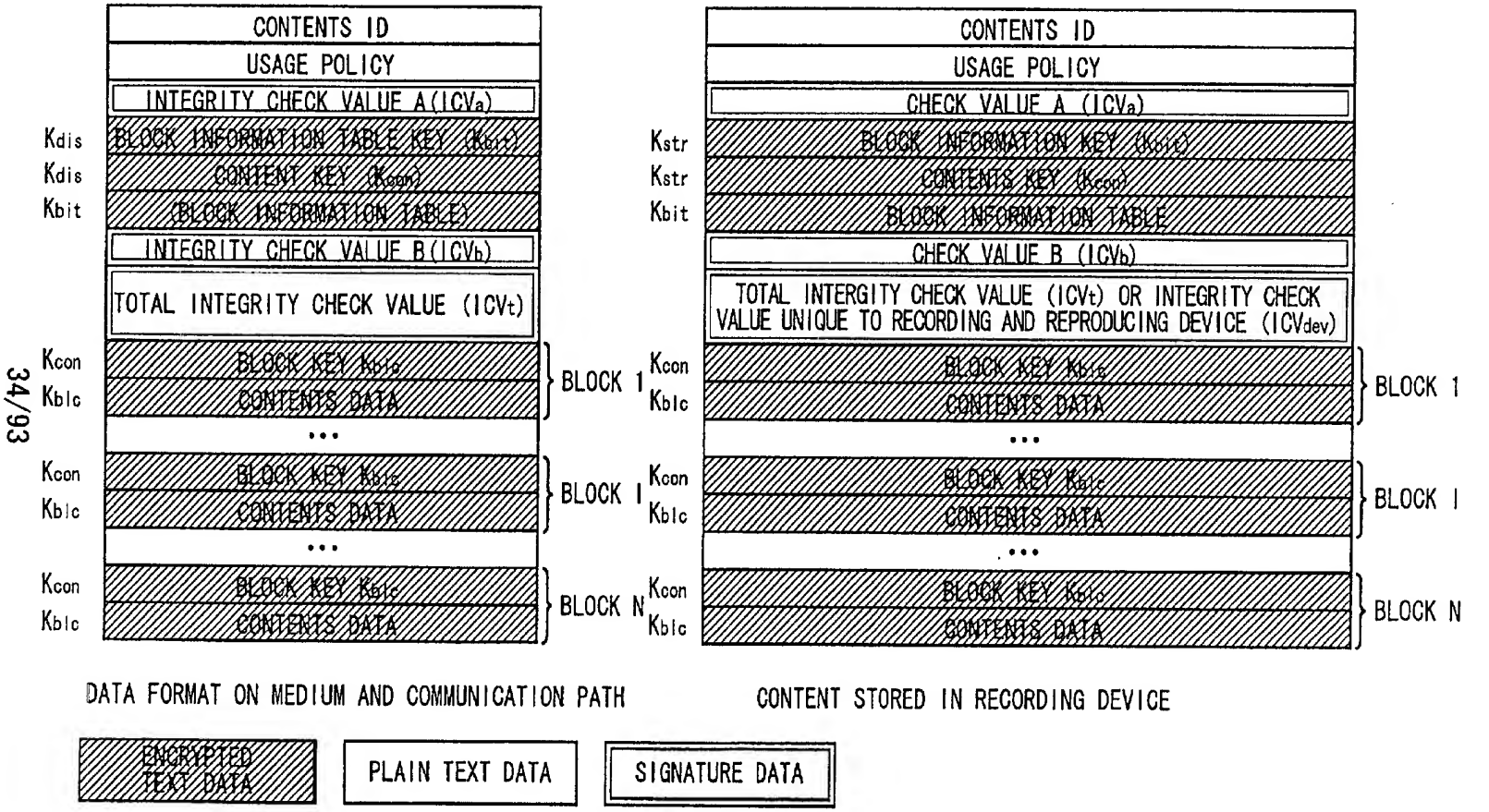


FIG. 34

FORMAT TYPE 3

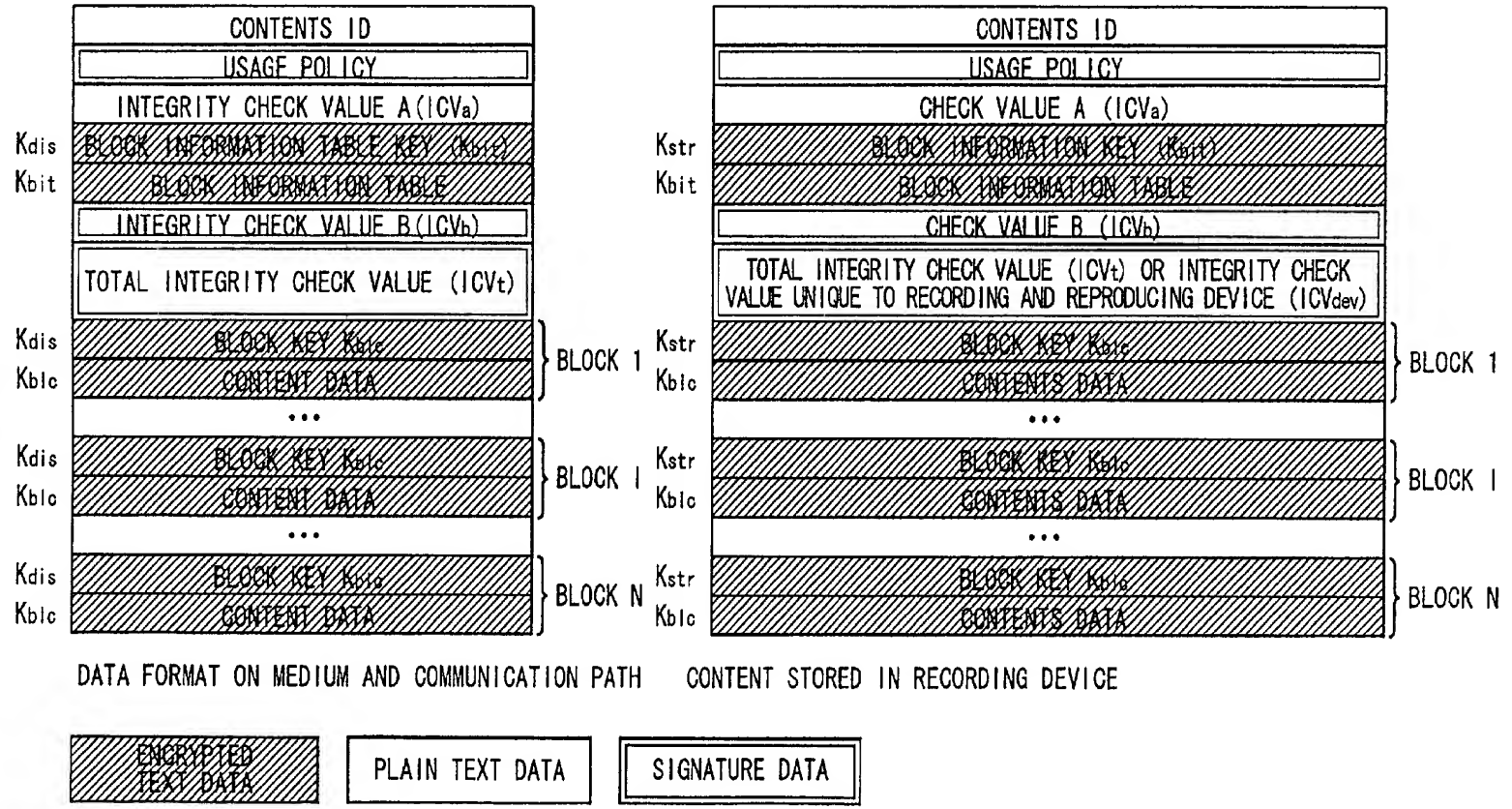
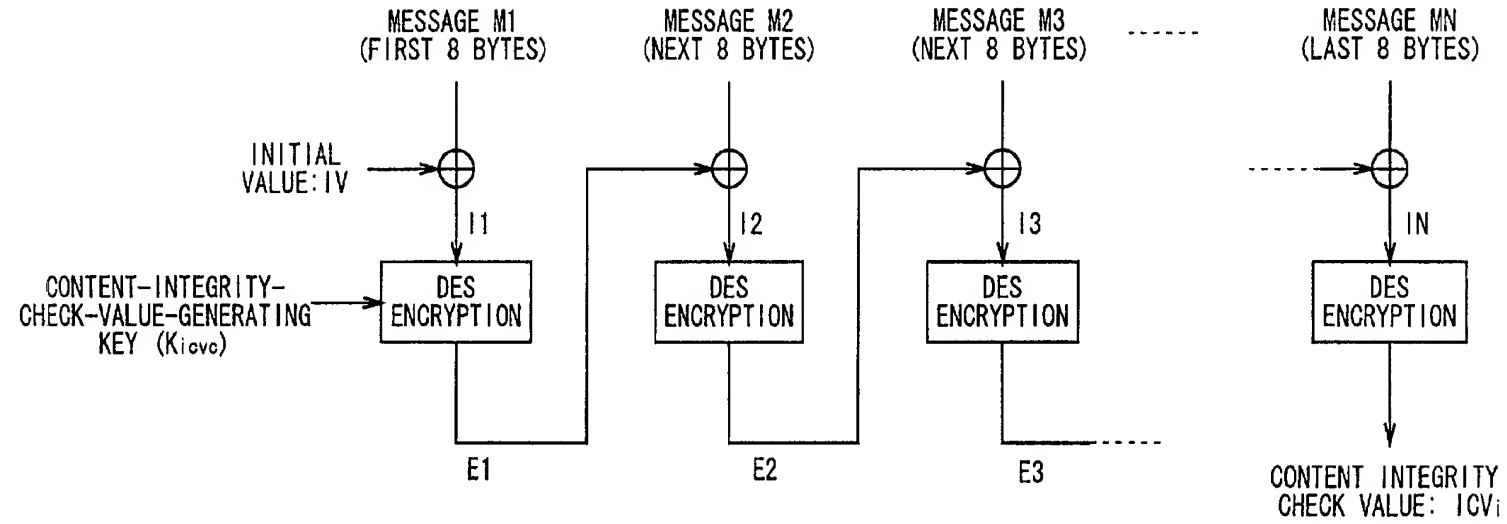


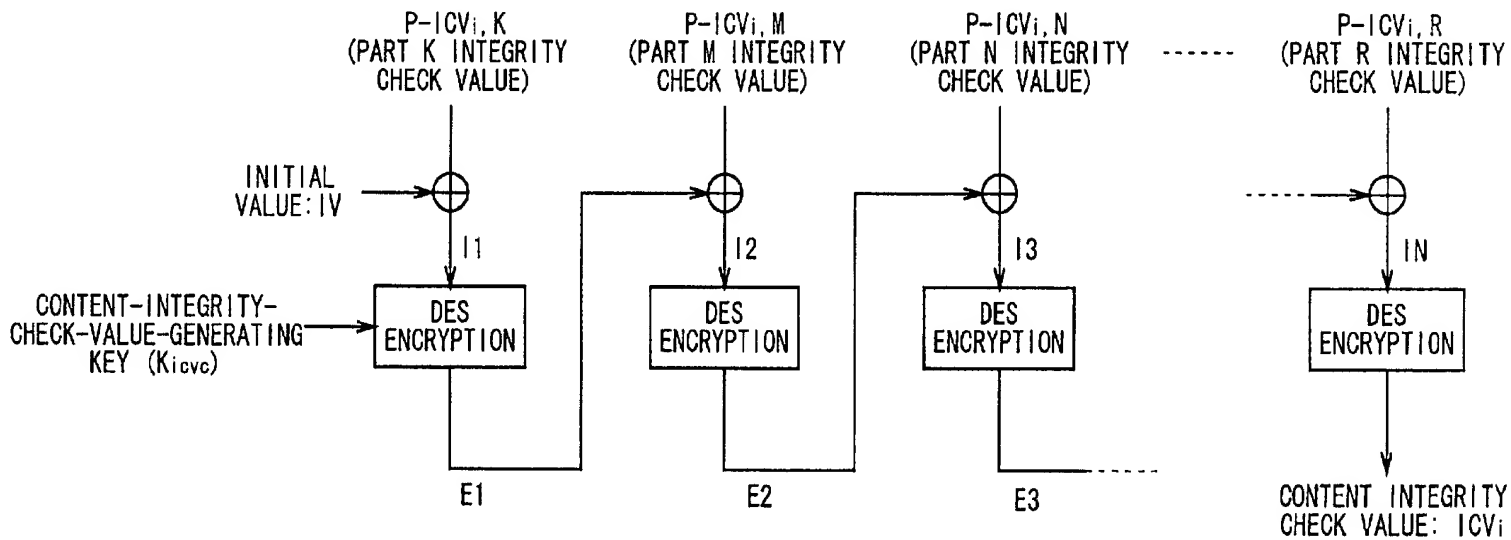
FIG. 35



MESSAGES M1 TO MN: CONTENT DATA IN CONTENT i

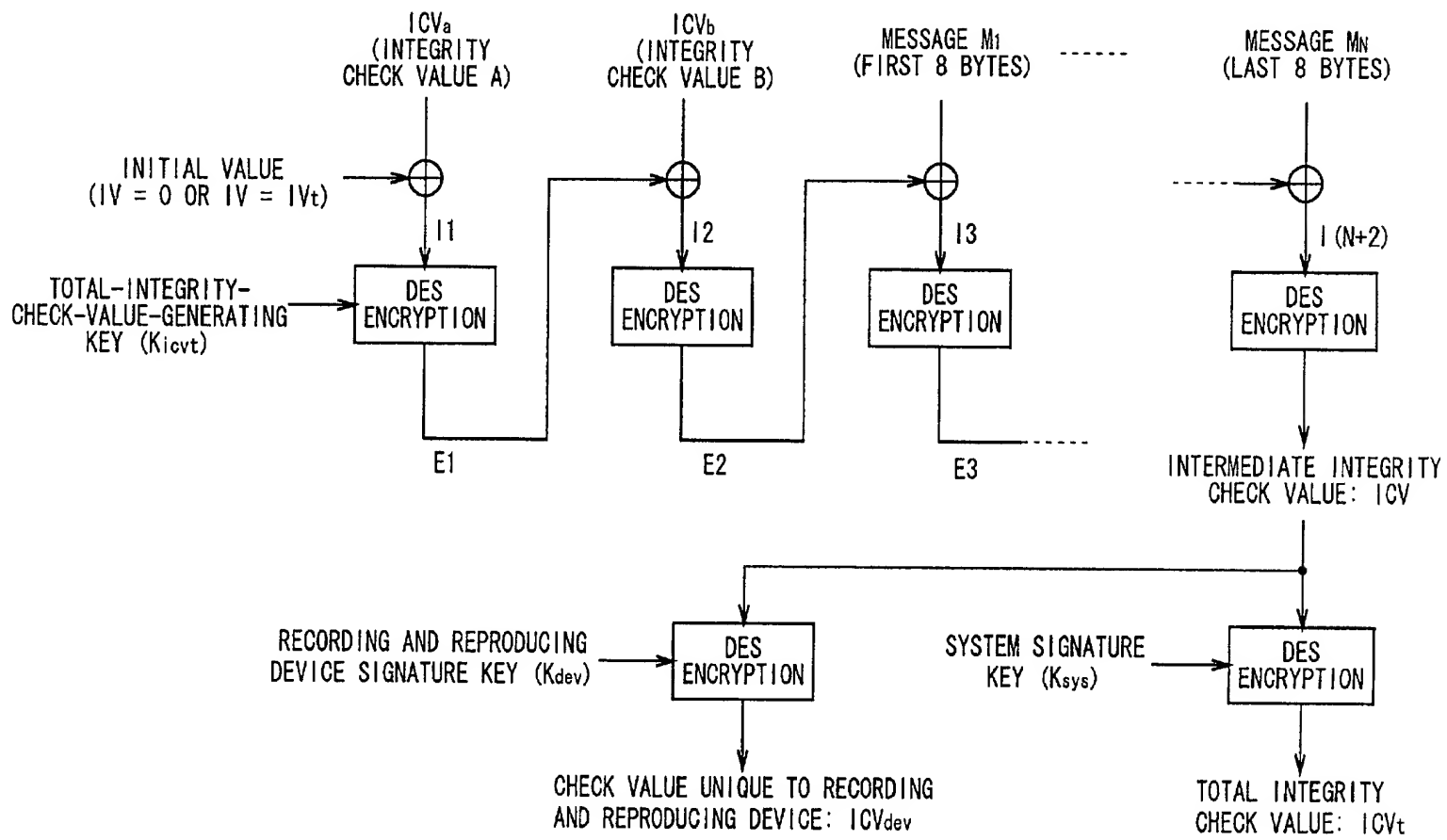
⊕:EXCLUSIVE OR PROCESS (EVERY 8 BYTES)

FIG. 36



⊕: EXCLUSIVE OR PROCESS (EVERY 8 BYTES)

FIG. 37



MESSAGES M1 TO MN: DATA IN CONTENT BLOCKS 1 TO N

⊕:EXCLUSIVE OR PROCESS (EVERY 8 BYTES)

FIG. 38

FORMAT TYPE 0 AND 1 DOWNLOAD PROCESS

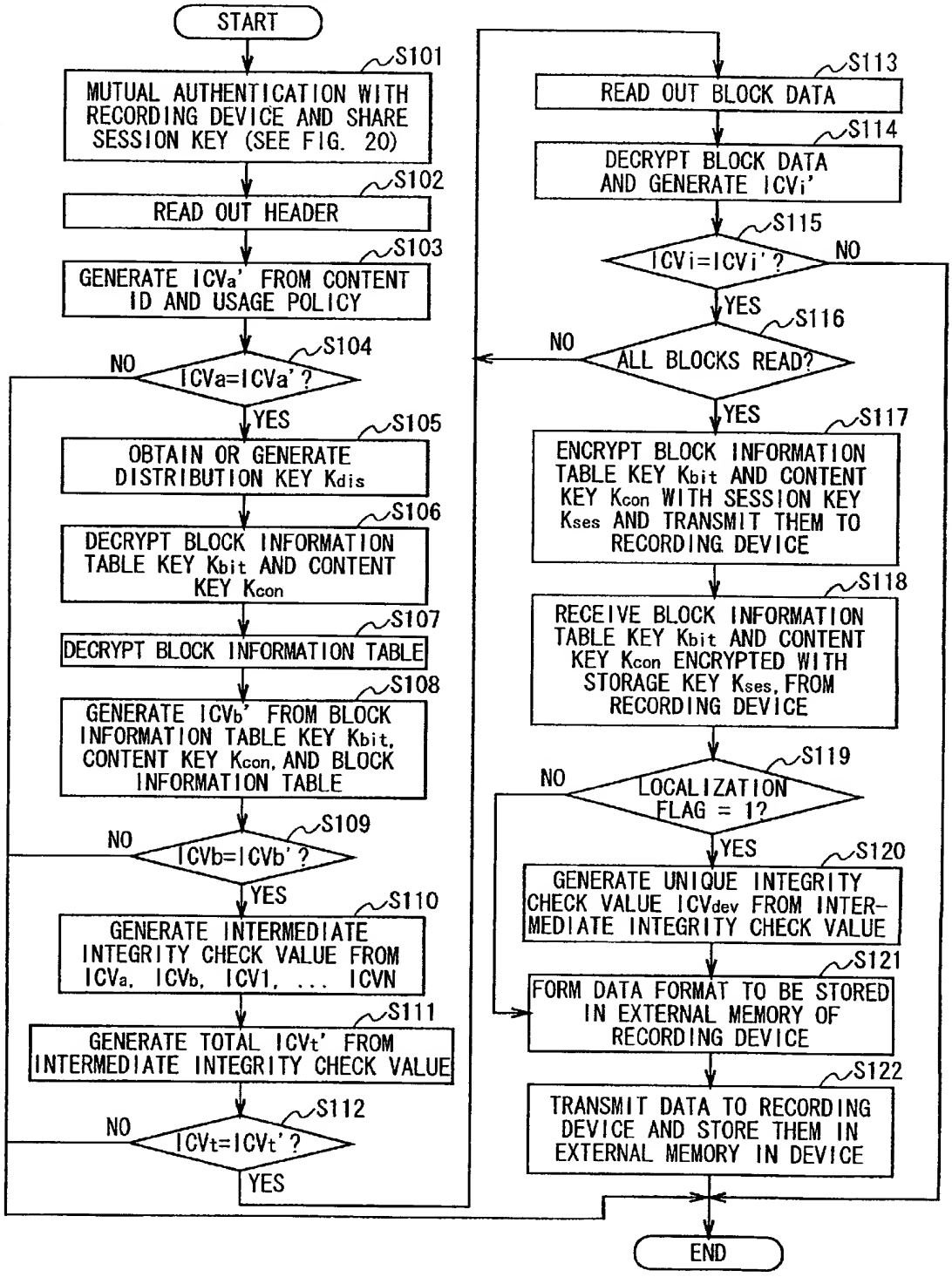


FIG. 39

FORMAT TYPE 2 DOWNLOAD PROCESS

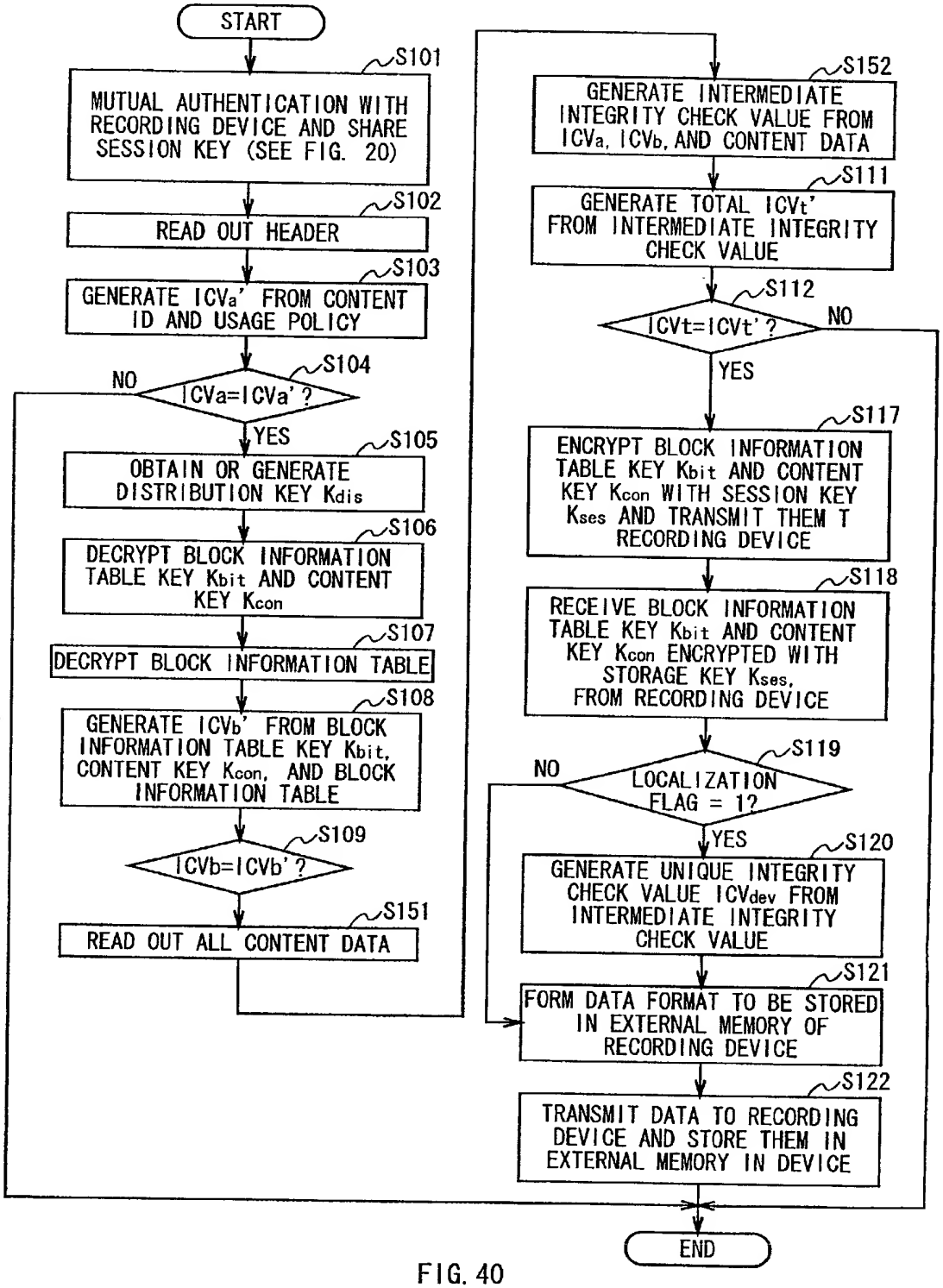


FIG. 40

FORMAT TYPE 3 DOWNLOAD PROCESS

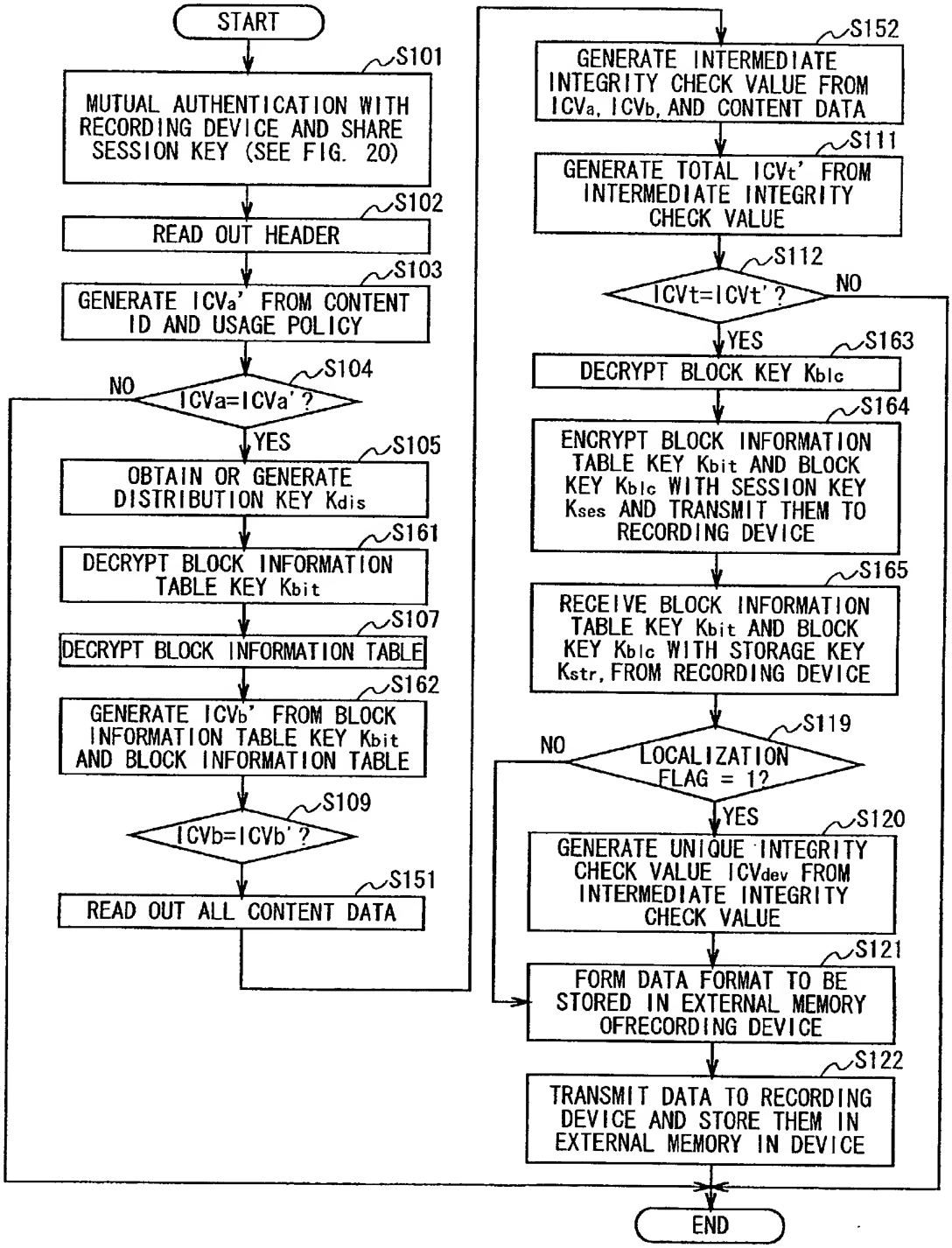


FIG. 41

FORMAT TYPE 0 REPRODUCTION PROCESS

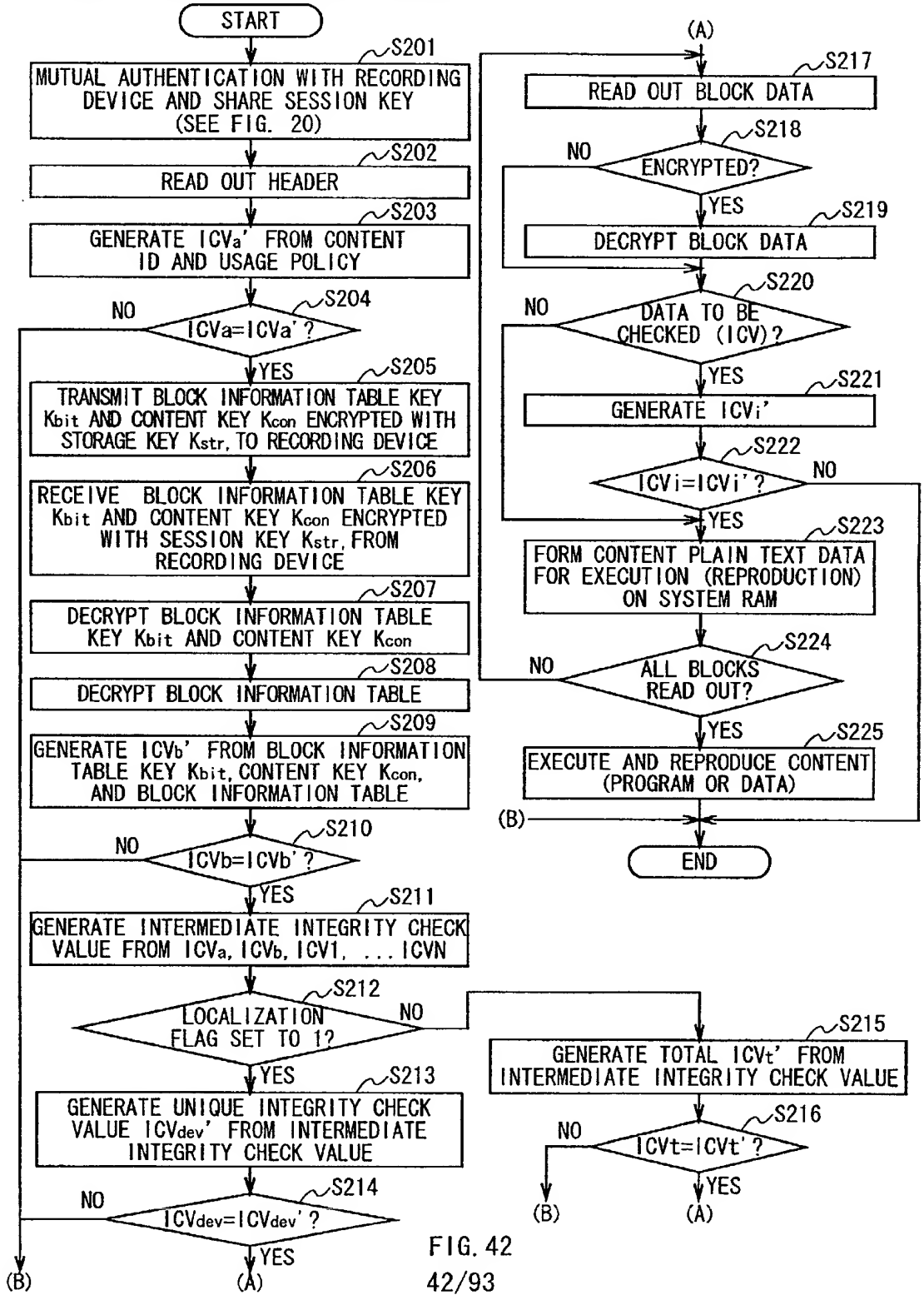


FIG. 42

FORMAT TYPE 1 REPRODUCTION PROCESS

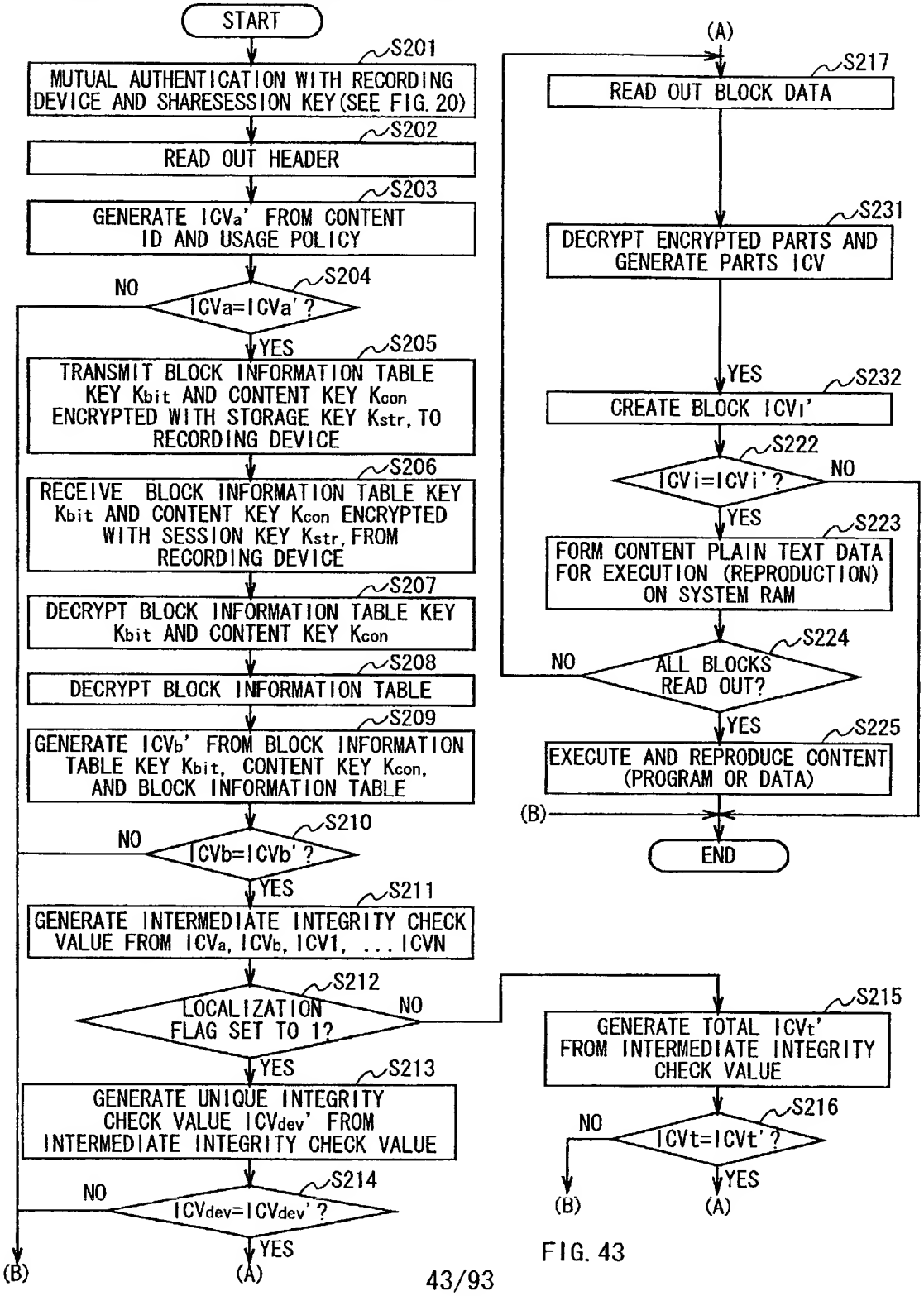


FIG. 43

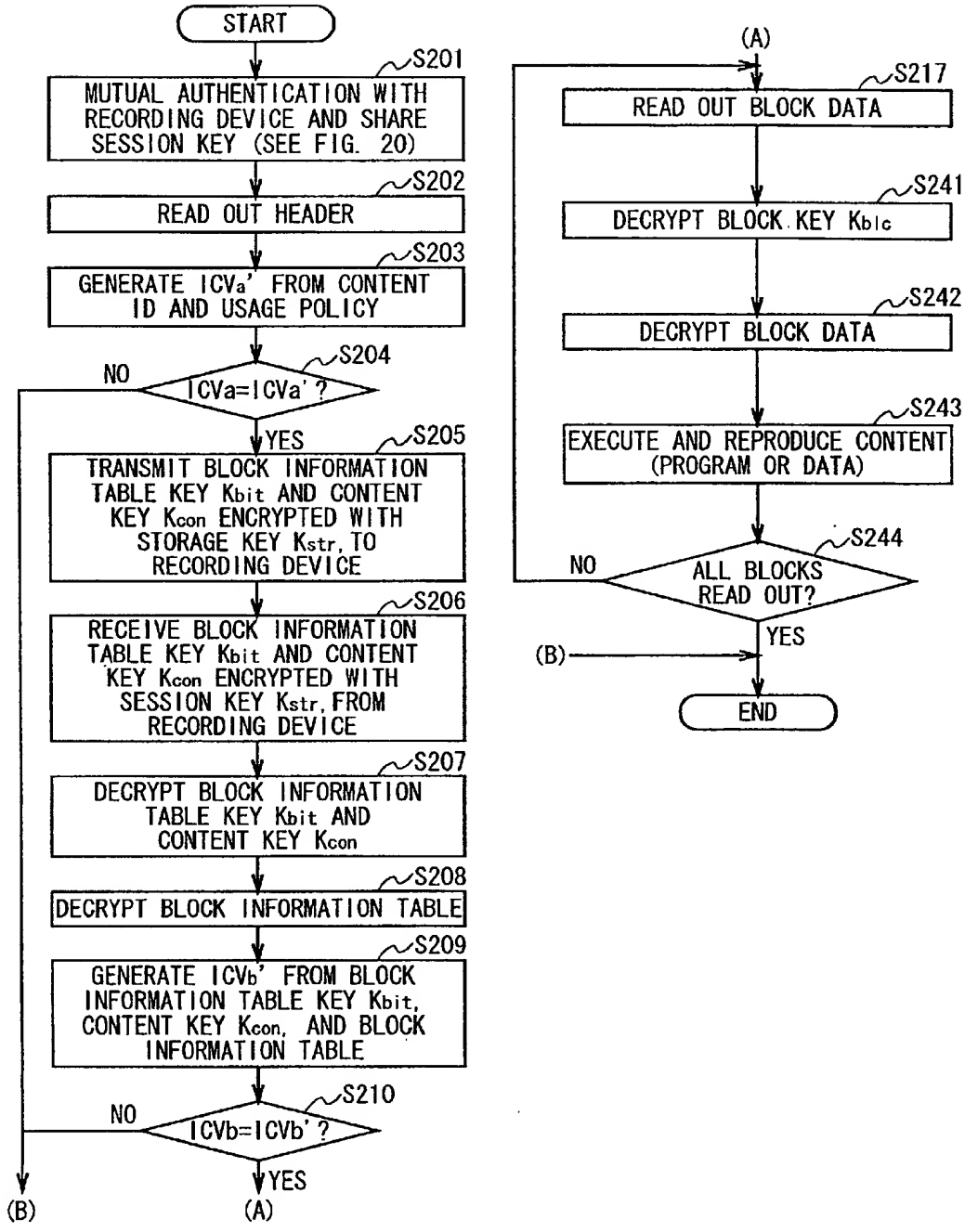

START
S201
MUTUAL AUTHENTICATION WITH RECORDING DEVICE AND SHARE SESSION KEY (SEE FIG. 20)
S202
READ OUT HEADER
S203
GENERATE ICVa' FROM CONTENT ID AND USAGE POLICY
S204
NO
ICVa=ICVa' ?
YES
S205
TRANSMIT BLOCK INFORMATION TABLE KEY Kbit AND CONTENT KEY Kcon ENCRYPTED WITH STORAGE KEY Kstr, TO RECORDING DEVICE
S206
RECEIVE BLOCK INFORMATION TABLE KEY Kbit AND CONTENT KEY Kcon ENCRYPTED WITH SESSION KEY Kstr, FROM RECORDING DEVICE
S207
DECRYPT BLOCK INFORMATION TABLE KEY Kbit AND CONTENT KEY Kcon
S208
DECRYPT BLOCK INFORMATION TABLE
S209
GENERATE ICVb' FROM BLOCK INFORMATION TABLE KEY Kbit, CONTENT KEY Kcon, AND BLOCK INFORMATION TABLE
S210
NO
ICVb=ICVb' ?
YES
(B)
(A)
(A)
S217
READ OUT BLOCK DATA
S241
DECRYPT BLOCK KEY Kblc
S242
DECRYPT BLOCK DATA
S243
EXECUTE AND REPRODUCE CONTENT (PROGRAM OR DATA)
S244
NO
ALL BLOCKS READ OUT?
YES
(B)
END

FIG. 44

FORMAT TYPE 3 REPRODUCTION PROCESS

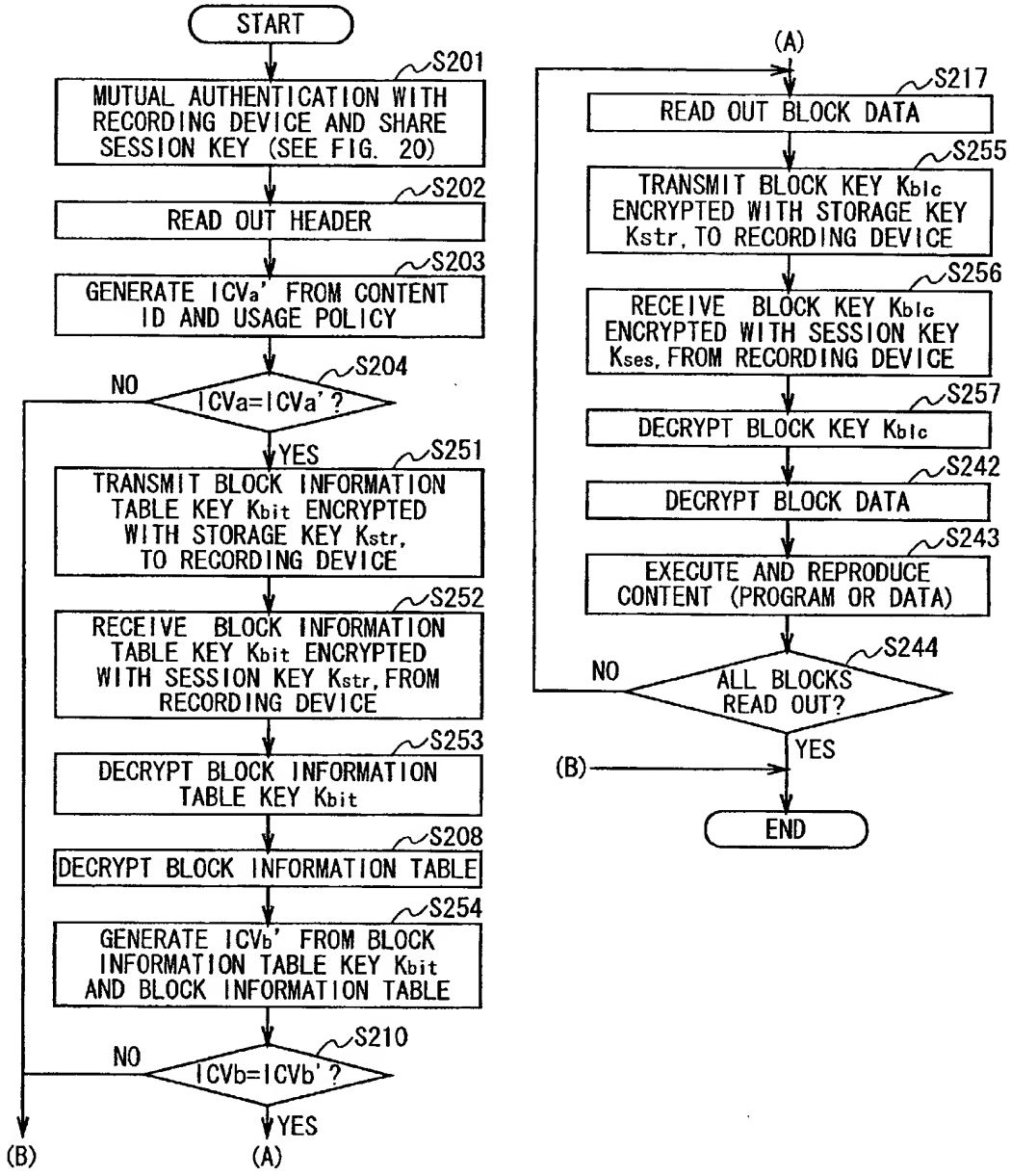


FIG. 45

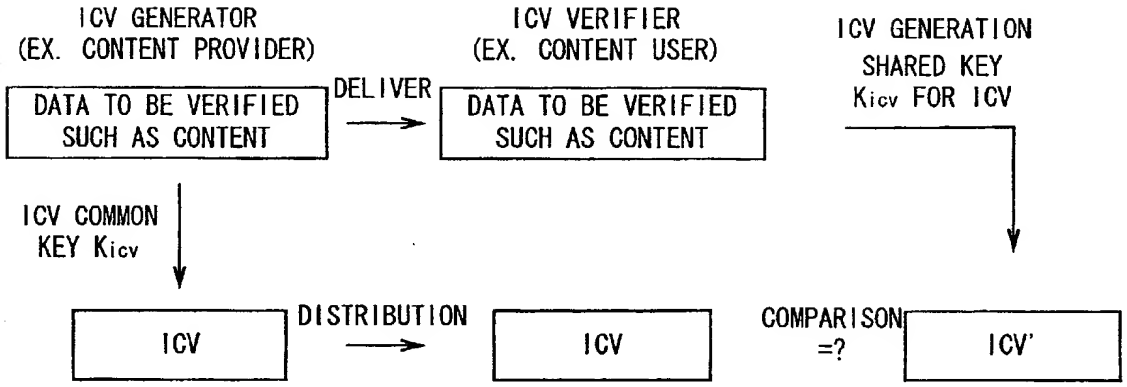

ICV GENERATOR
(EX. CONTENT PROVIDER)
ICV VERIFIER
(EX. CONTENT USER)
ICV GENERATION
SHARED KEY
Kicv FOR ICV
DATA TO BE VERIFIED
SUCH AS CONTENT
DELIVER
DATA TO BE VERIFIED
SUCH AS CONTENT
ICV COMMON
KEY Kicv
ICV
DISTRIBUTION
ICV
COMPARISON
=?
ICV'

FIG. 46

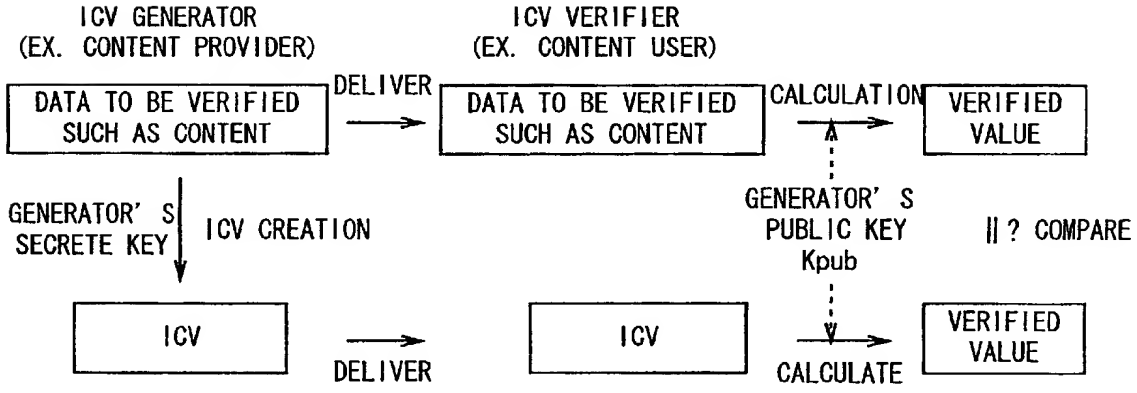

ICV GENERATOR
(EX. CONTENT PROVIDER)
ICV VERIFIER
(EX. CONTENT USER)
DATA TO BE VERIFIED
SUCH AS CONTENT
DELIVER
DATA TO BE VERIFIED
SUCH AS CONTENT
CALCULATION
VERIFIED
VALUE
GENERATOR' S
SECRETE KEY
ICV CREATION
GENERATOR' S
PUBLIC KEY
Kpub
|| ? COMPARE
ICV
DELIVER
ICV
CALCULATE
VERIFIED
VALUE

FIG. 47

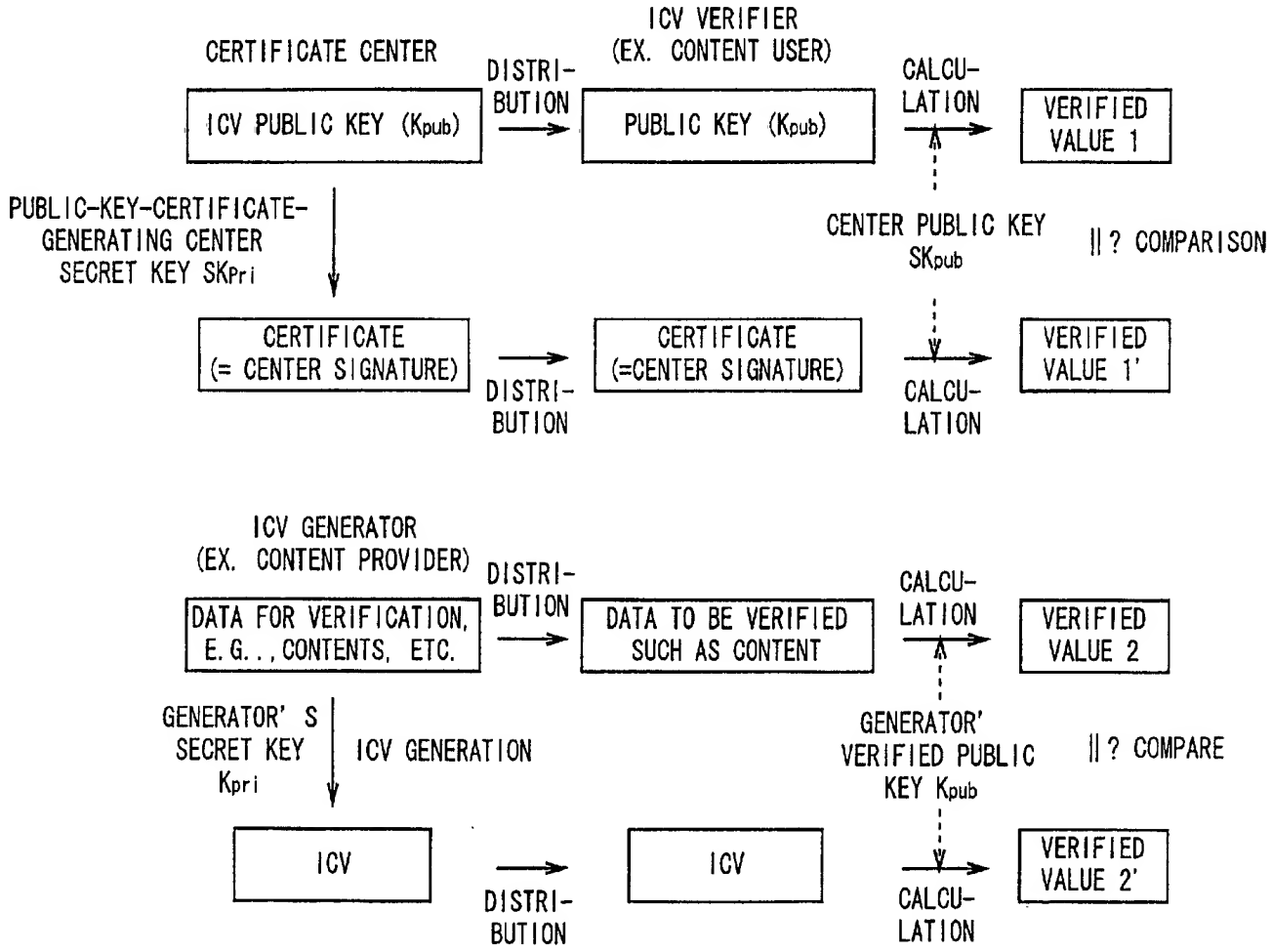
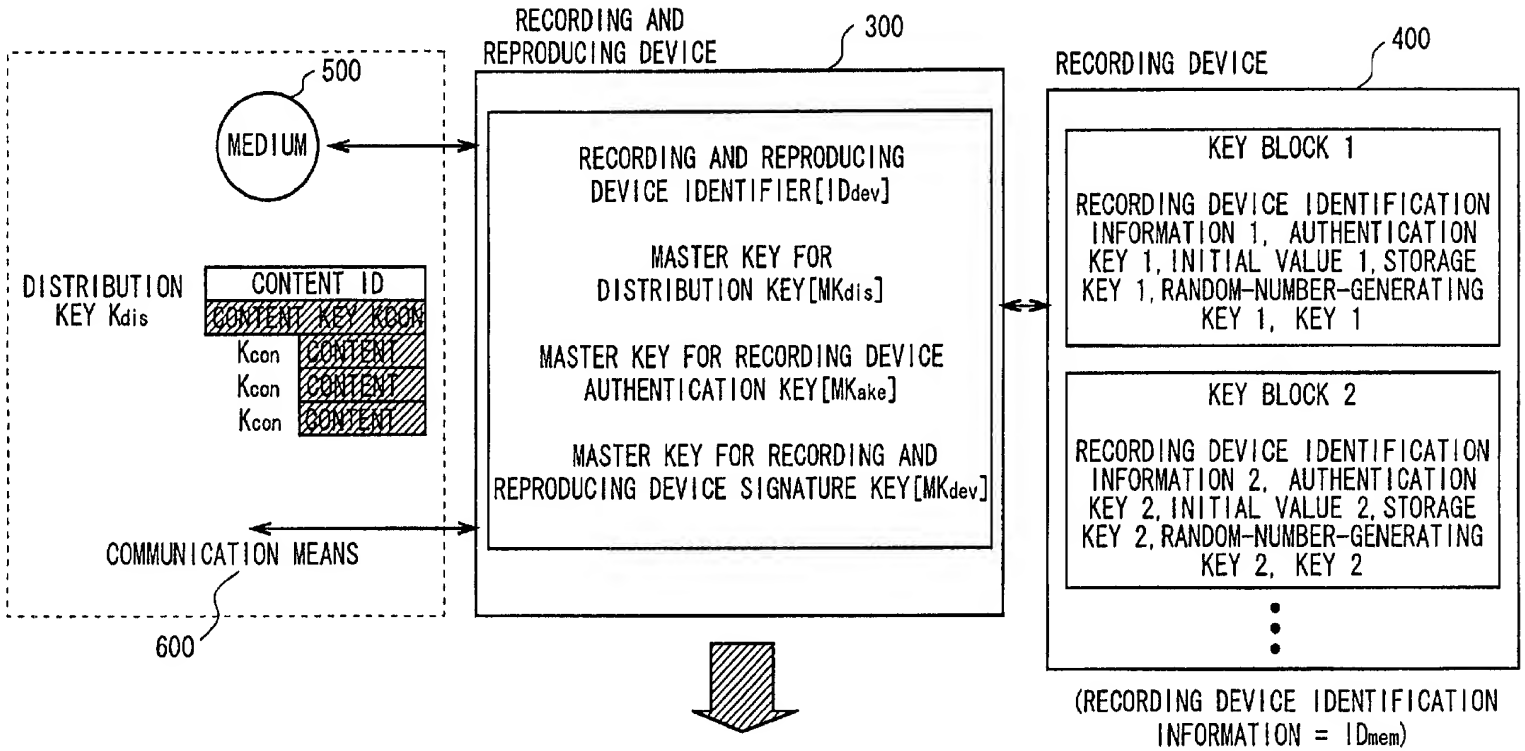


FIG. 48



DISTRIBUTION KEY : K_{DIS} = DES (MK_{dis}, CONTENT ID)

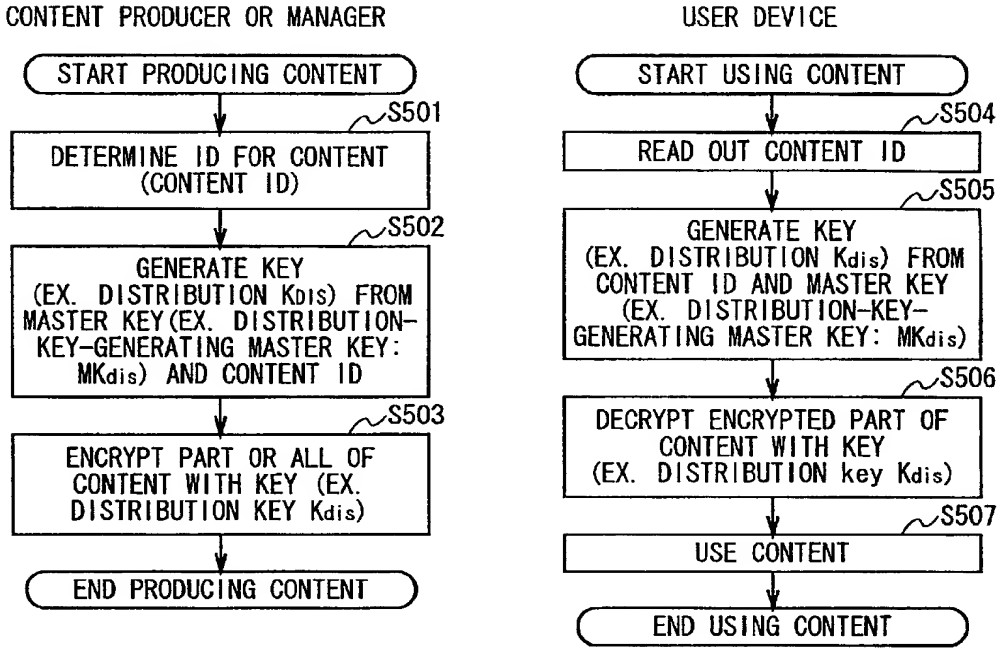
AUTHENTICATION KEY : K_{ake} = DES (MK_{ake}, ID_{mem})

RECORDING AND REPRODUCING DEVICE SIGNATURE KEY : K_{dev} = DES (MK_{dev}, ID_{dev})

FIG. 49

METHOD FOR GENERATING INDIVIDUAL KEY FROM MASTER KEY -(1)

[BASIC FLOW]



[KEY OWNER CONFIGURATION]

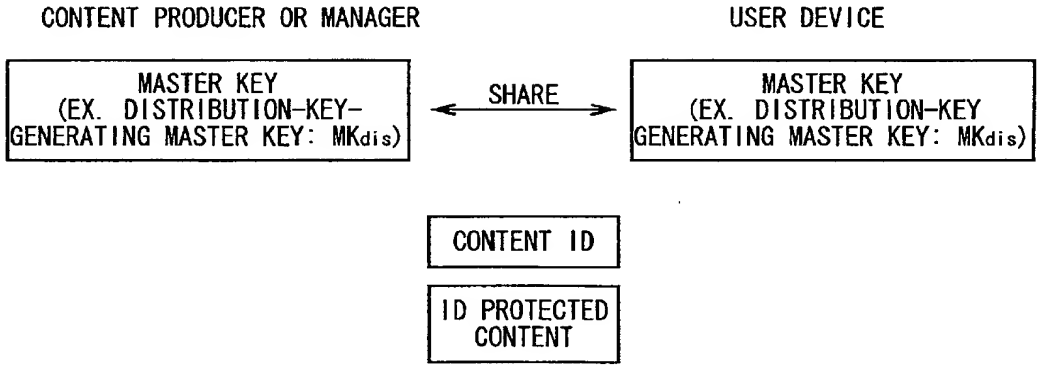
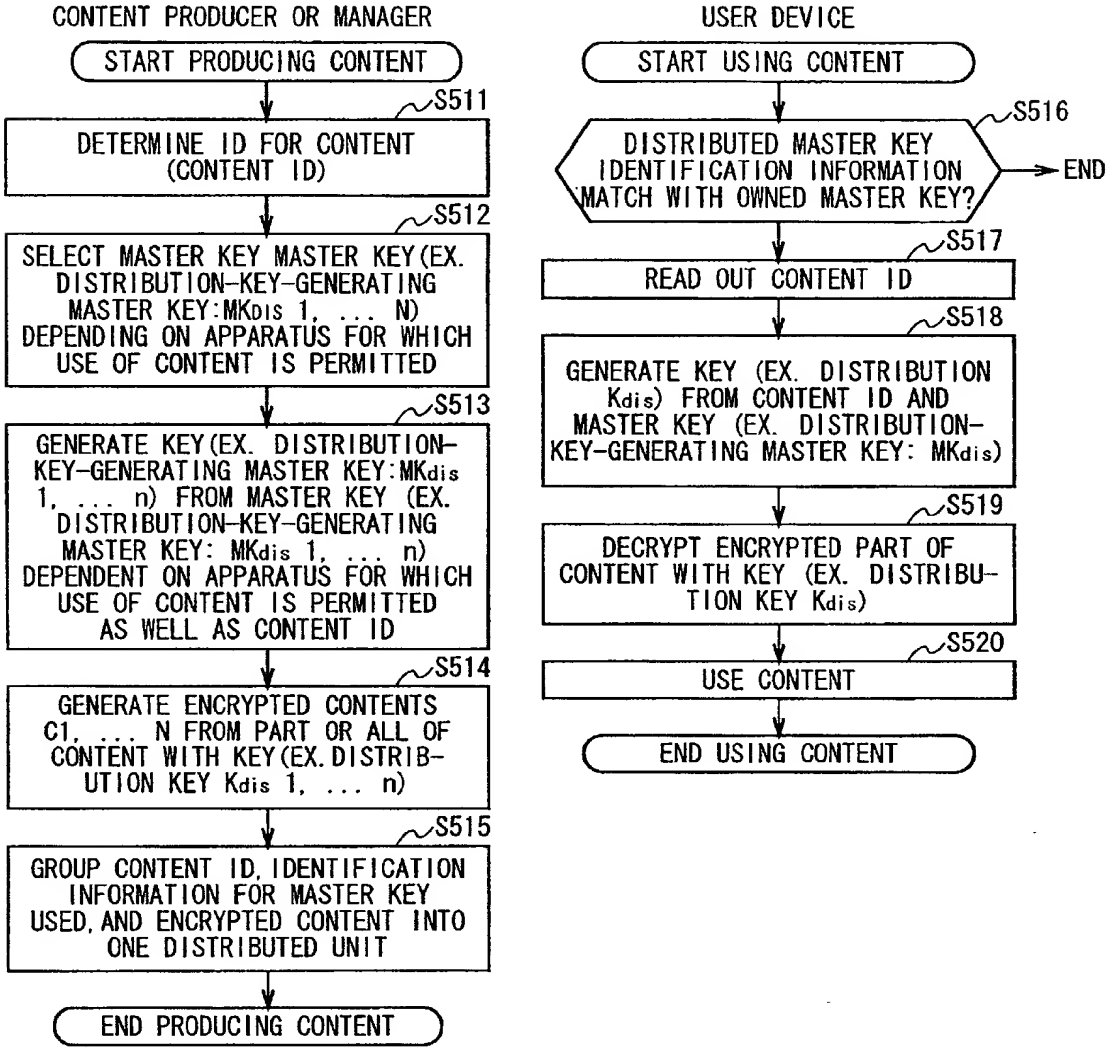


FIG. 50

METHOD FOR GENERATING INDIVIDUAL KEY FROM MASTER KEY -(2)

[BASIC FLOW]



[KEY OWNER CONFIGURATION]

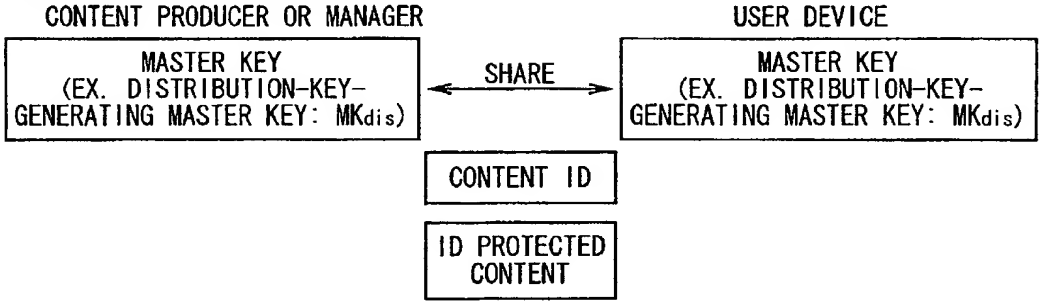


FIG. 51

CONTENT PROVIDER OR MANAGER

MASTER KEY	TERRITORY	ENCRYPTION KEY	ENCRYPTION (CONTENT)
MK1	JAPAN	(MK1, CONTENT ID)→K1	K1 (CONTENT)
MK2	U.S.	(MK2, CONTENT ID)→K2	K2 (CONTENT)
MK3	EU	(MK3, CONTENT ID)→K3	K3 (CONTENT)
MK4	:	:	:
:	:	:	:

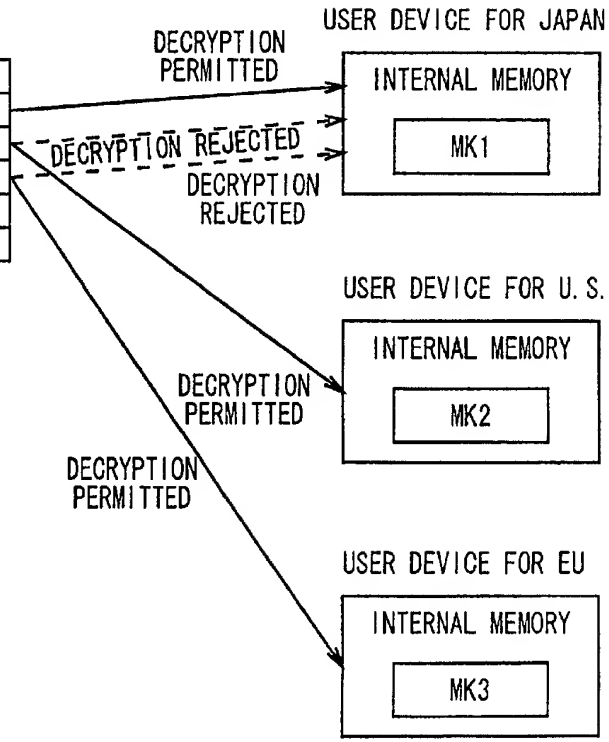
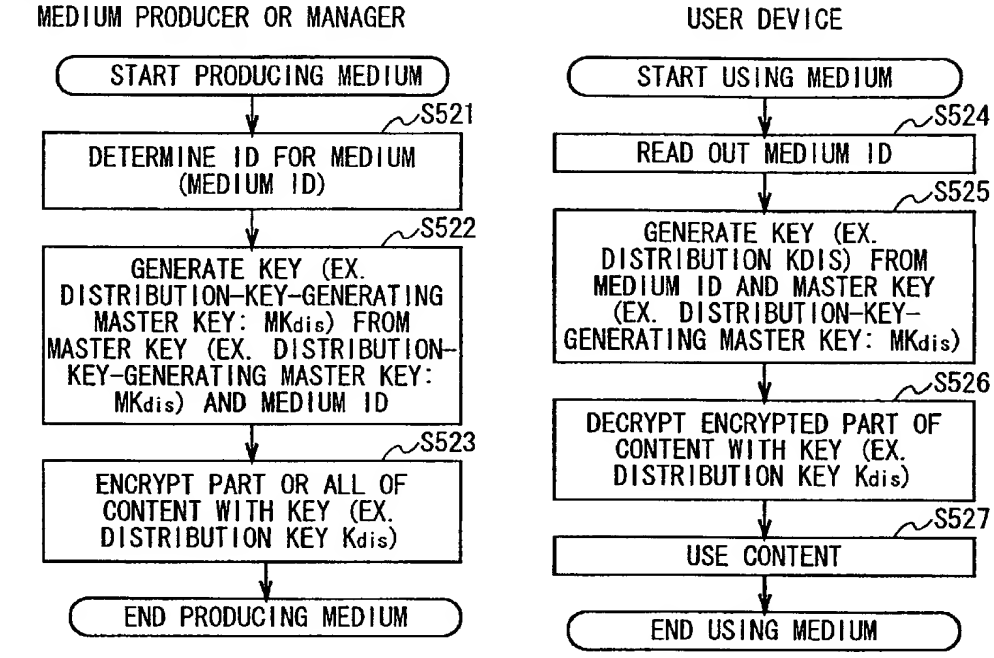


FIG. 52

METHOD FOR GENERATING INDIVIDUAL KEY FROM MASTER KEY -(3)

[BASIC FLOW]



[KEY OWNER CONFIGURATION]

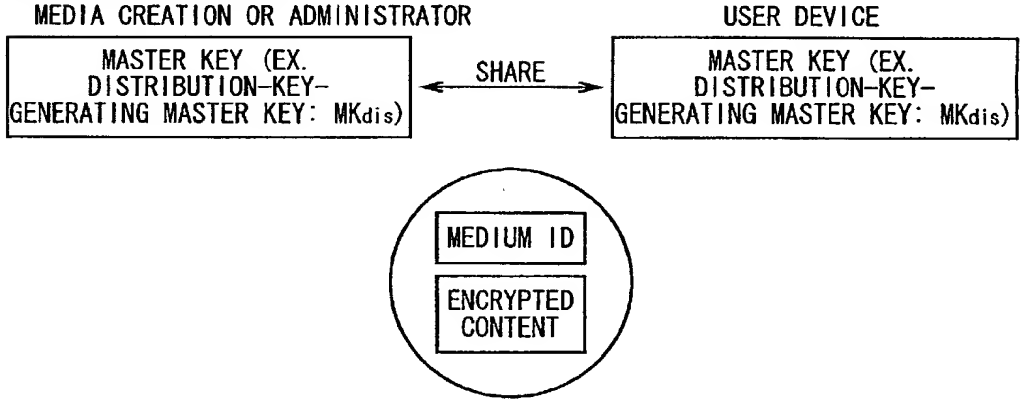
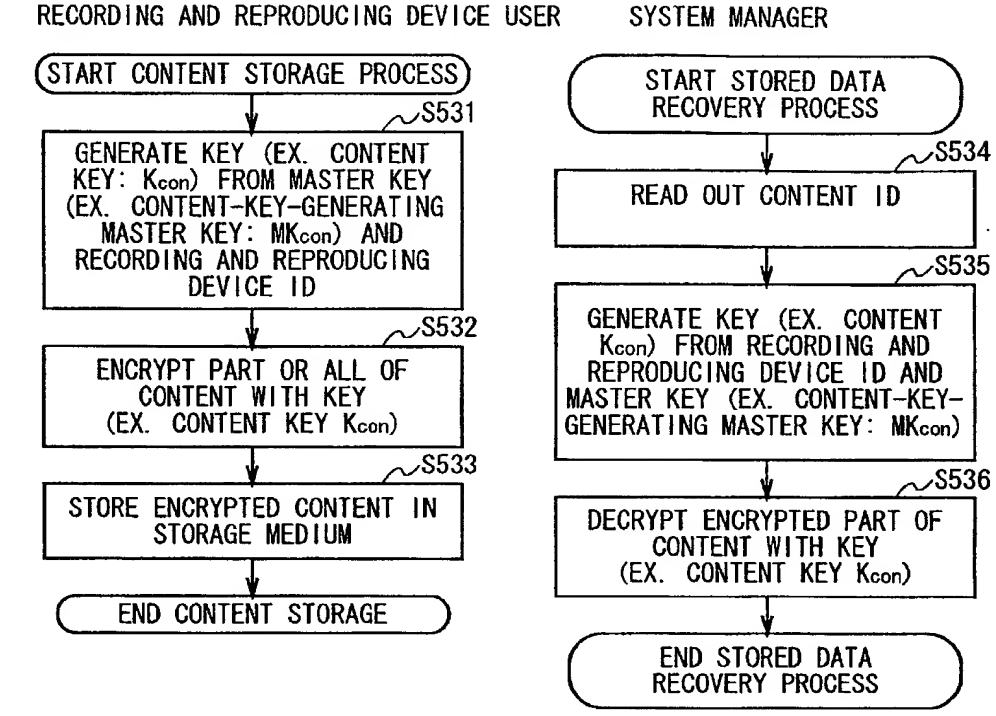


FIG. 53

METHOD FOR GENERATING INDIVIDUAL KEY FROM MASTER KEY -(4)

[BASIC FLOW]



[KEY OWNER CONFIGURATION]

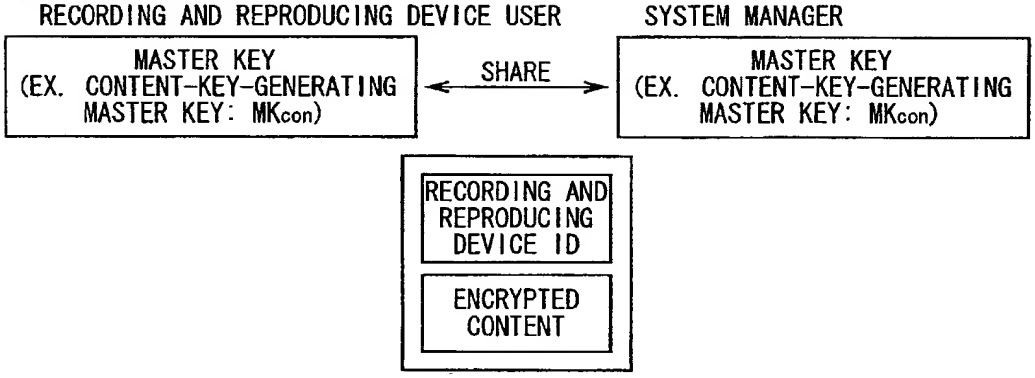
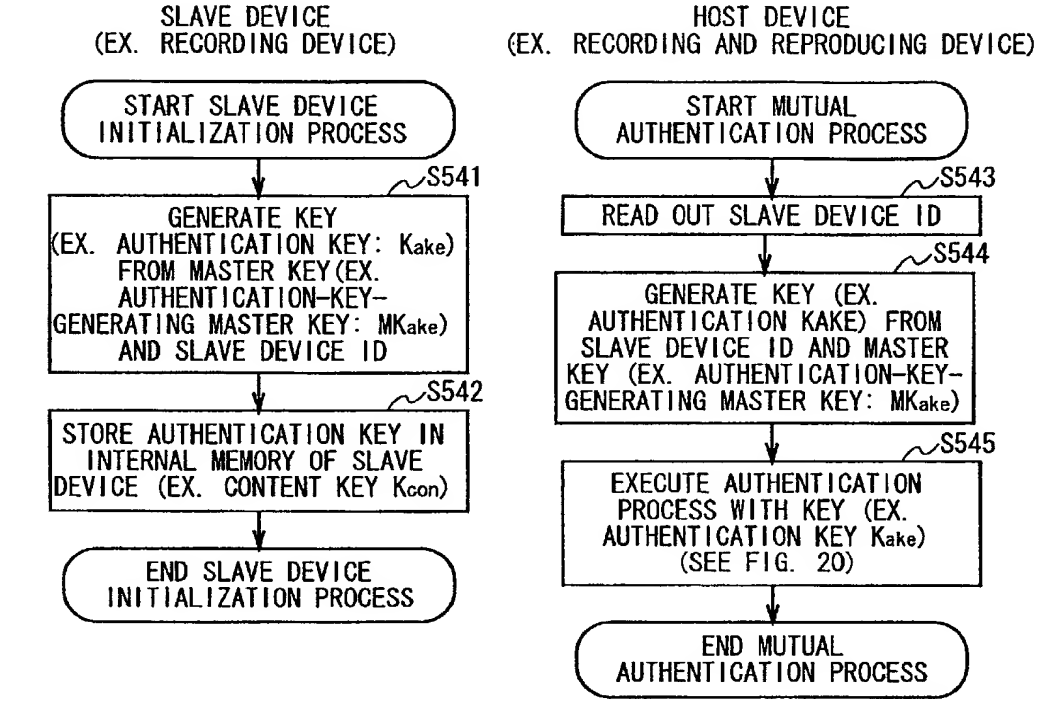


FIG. 54

METHOD FOR GENERATING INDIVIDUAL KEY FROM MASTER KEY - (5)

[BASIC FLOW]



[KEY OWNER CONFIGURATION]

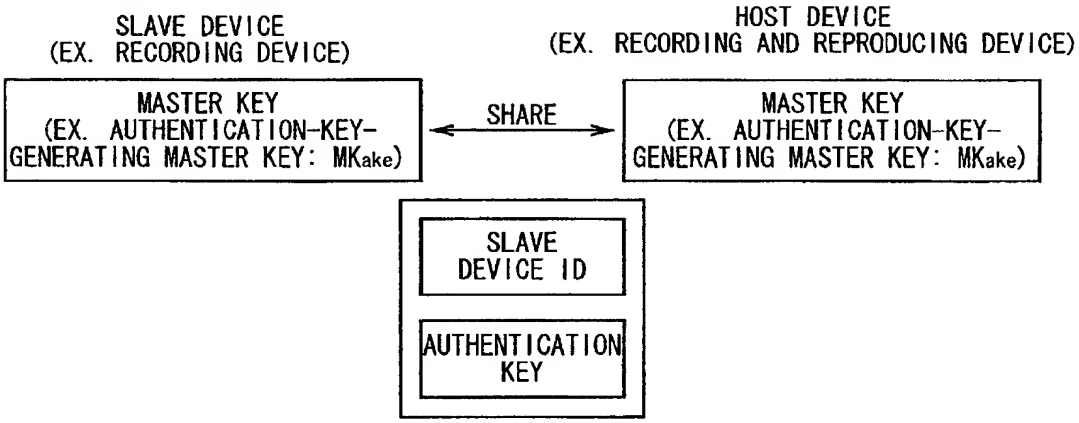


FIG. 55

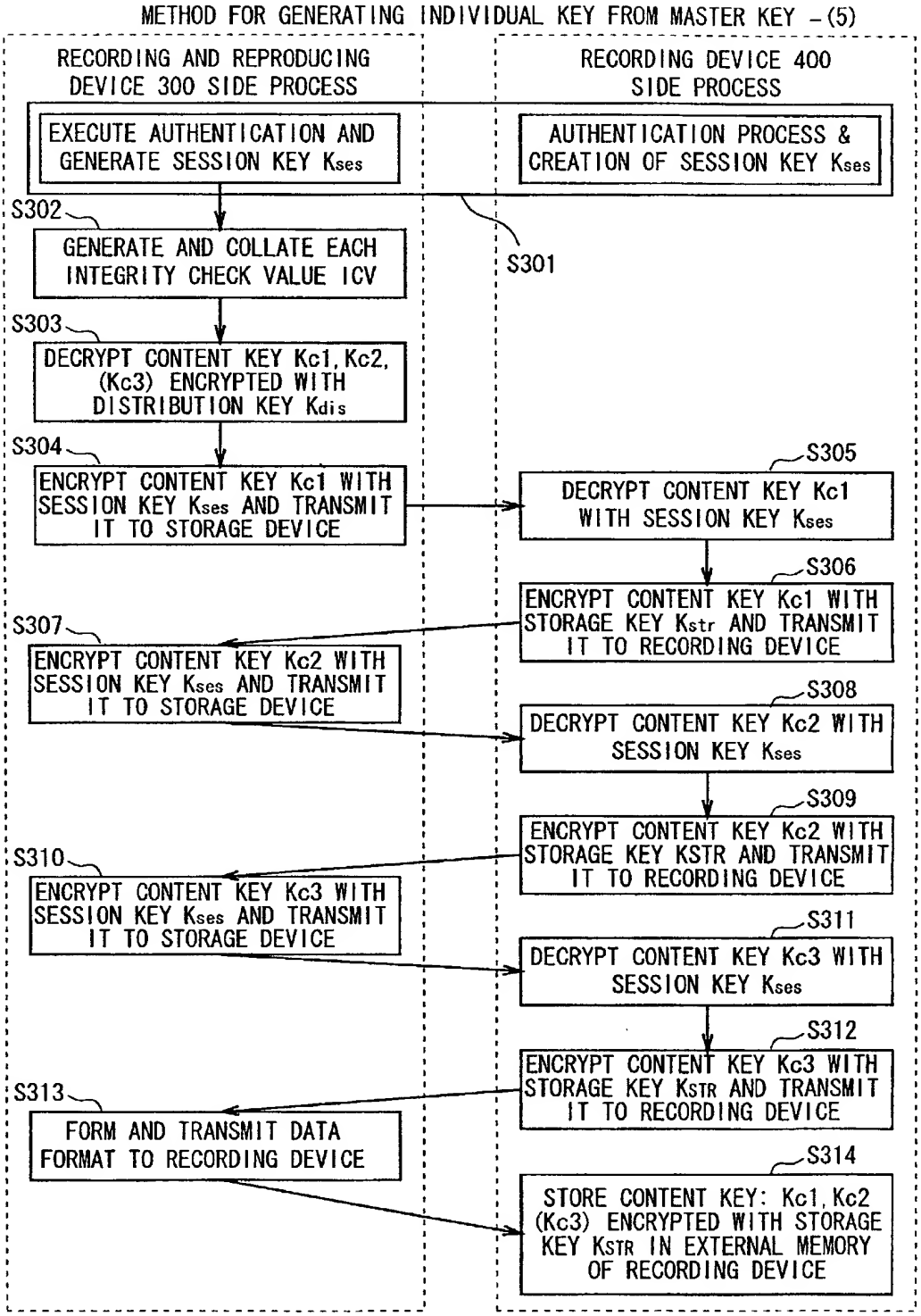

METHOD FOR GENERATING INDIVIDUAL KEY FROM MASTER KEY -(5)
RECORDING AND REPRODUCING DEVICE 300 SIDE PROCESS
RECORDING DEVICE 400 SIDE PROCESS
EXECUTE AUTHENTICATION AND GENERATE SESSION KEY Kses
AUTHENTICATION PROCESS & CREATION OF SESSION KEY Kses
S301
S302
GENERATE AND COLLATE EACH INTEGRITY CHECK VALUE ICV
S303
DECRYPT CONTENT KEY Kc1, Kc2, (Kc3) ENCRYPTED WITH DISTRIBUTION KEY Kdis
S304
ENCRYPT CONTENT KEY Kc1 WITH SESSION KEY Kses AND TRANSMIT IT TO STORAGE DEVICE
S305
DECRYPT CONTENT KEY Kc1 WITH SESSION KEY Kses
S306
ENCRYPT CONTENT KEY Kc1 WITH STORAGE KEY Kstr AND TRANSMIT IT TO RECORDING DEVICE
S307
ENCRYPT CONTENT KEY Kc2 WITH SESSION KEY Kses AND TRANSMIT IT TO STORAGE DEVICE
S308
DECRYPT CONTENT KEY Kc2 WITH SESSION KEY Kses
S309
ENCRYPT CONTENT KEY Kc2 WITH STORAGE KEY KSTR AND TRANSMIT IT TO RECORDING DEVICE
S310
ENCRYPT CONTENT KEY Kc3 WITH SESSION KEY Kses AND TRANSMIT IT TO STORAGE DEVICE
S311
DECRYPT CONTENT KEY Kc3 WITH SESSION KEY Kses
S312
ENCRYPT CONTENT KEY Kc3 WITH STORAGE KEY KSTR AND TRANSMIT IT TO RECORDING DEVICE
S313
FORM AND TRANSMIT DATA FORMAT TO RECORDING DEVICE
S314
STORE CONTENT KEY: Kc1, Kc2 (Kc3) ENCRYPTED WITH STORAGE KEY KSTR IN EXTERNAL MEMORY OF RECORDING DEVICE

FIG. 56

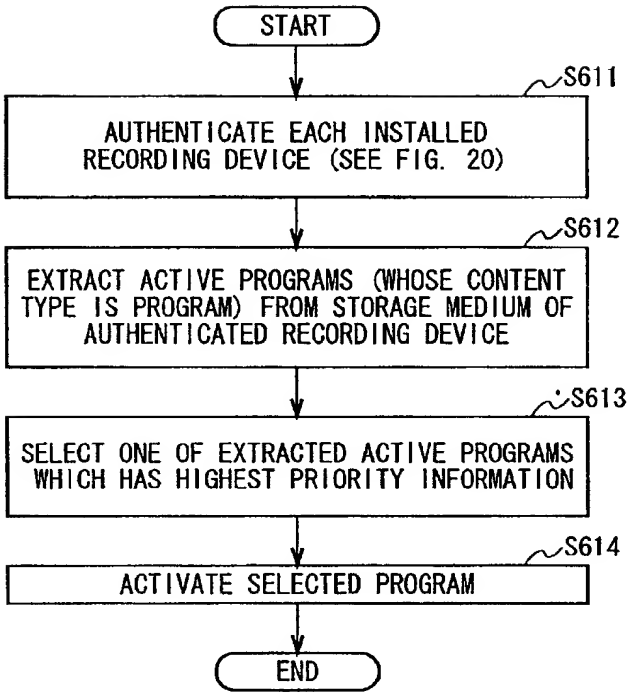

START
S611
AUTHENTICATE EACH INSTALLED RECORDING DEVICE (SEE FIG. 20)
S612
EXTRACT ACTIVE PROGRAMS (WHOSE CONTENT TYPE IS PROGRAM) FROM STORAGE MEDIUM OF AUTHENTICATED RECORDING DEVICE
S613
SELECT ONE OF EXTRACTED ACTIVE PROGRAMS WHICH HAS HIGHEST PRIORITY INFORMATION
S614
ACTIVATE SELECTED PROGRAM
END

FIG. 57

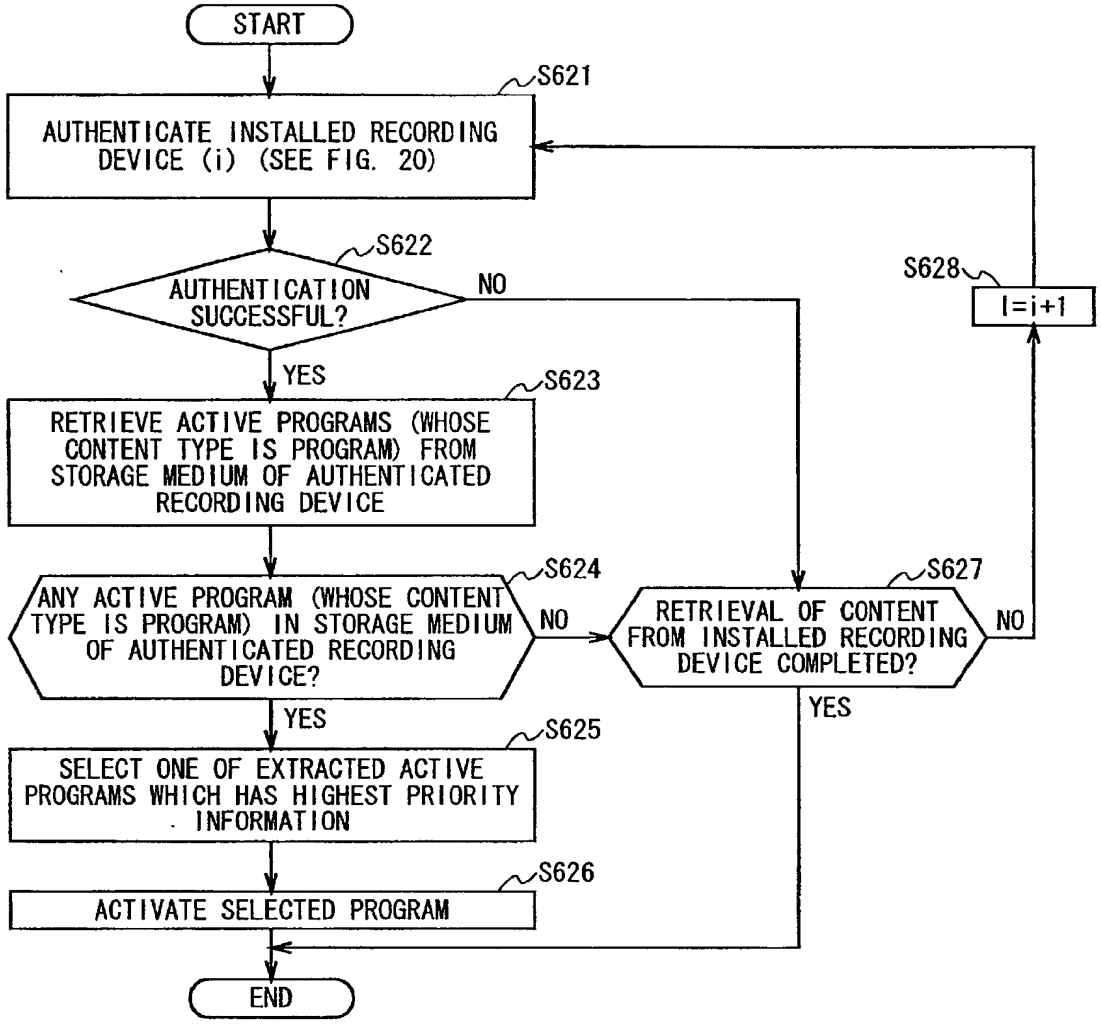

START
S621
AUTHENTICATE INSTALLED RECORDING DEVICE (i) (SEE FIG. 20)
S622
AUTHENTICATION SUCCESSFUL?
NO
YES
S623
RETRIEVE ACTIVE PROGRAMS (WHOSE CONTENT TYPE IS PROGRAM) FROM STORAGE MEDIUM OF AUTHENTICATED RECORDING DEVICE
S624
ANY ACTIVE PROGRAM (WHOSE CONTENT TYPE IS PROGRAM) IN STORAGE MEDIUM OF AUTHENTICATED RECORDING DEVICE?
NO
YES
S625
SELECT ONE OF EXTRACTED ACTIVE PROGRAMS WHICH HAS HIGHEST PRIORITY INFORMATION
S626
ACTIVATE SELECTED PROGRAM
END
S627
RETRIEVAL OF CONTENT FROM INSTALLED RECORDING DEVICE COMPLETED?
NO
YES
S628
I=i+1

FIG. 58

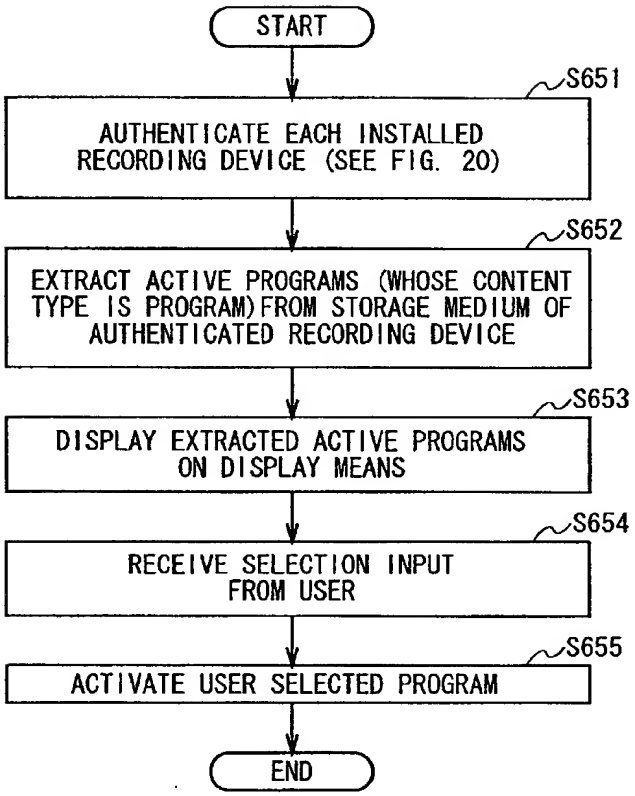

START
S651
AUTHENTICATE EACH INSTALLED RECORDING DEVICE (SEE FIG. 20)
S652
EXTRACT ACTIVE PROGRAMS (WHOSE CONTENT TYPE IS PROGRAM) FROM STORAGE MEDIUM OF AUTHENTICATED RECORDING DEVICE
S653
DISPLAY EXTRACTED ACTIVE PROGRAMS ON DISPLAY MEANS
S654
RECEIVE SELECTION INPUT FROM USER
S655
ACTIVATE USER SELECTED PROGRAM
END

FIG. 59

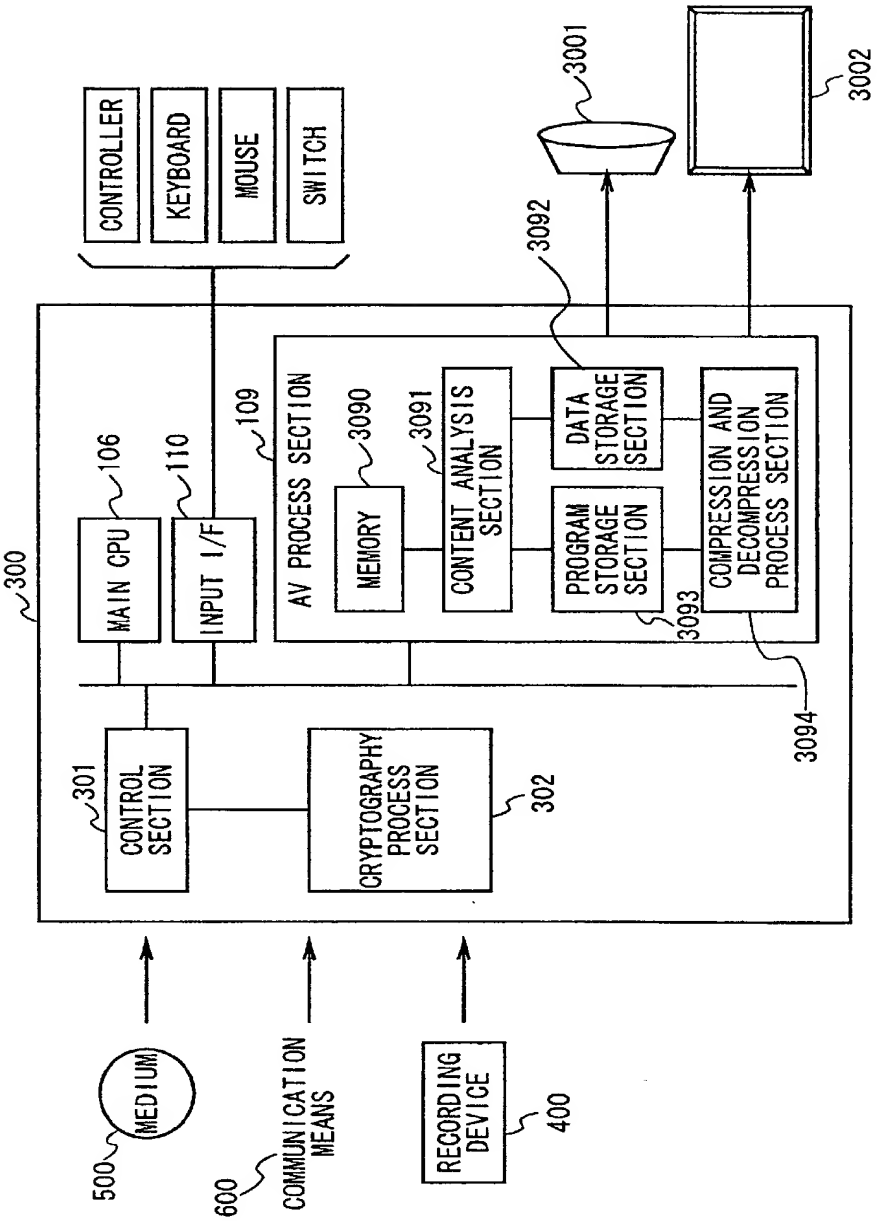

CONTROLLER
KEYBOARD
MOUSE
SWITCH
3001
3002
3092
300
MAIN CPU
106
INPUT I/F
110
109
AV PROCESS SECTION
MEMORY
3090
CONTENT ANALYSIS SECTION
3091
DATA STORAGE SECTION
PROGRAM STORAGE SECTION
3093
COMPRESSION AND DECOMPRESSION PROCESS SECTION
3094
301
CONTROL SECTION
CRYPTOGRAPHY PROCESS SECTION
302
MEDIUM
500
COMMUNICATION MEANS
600
RECORDING DEVICE
400

FIG. 60

EXAMPLE OF CONTENT CONFIGURATION (1)

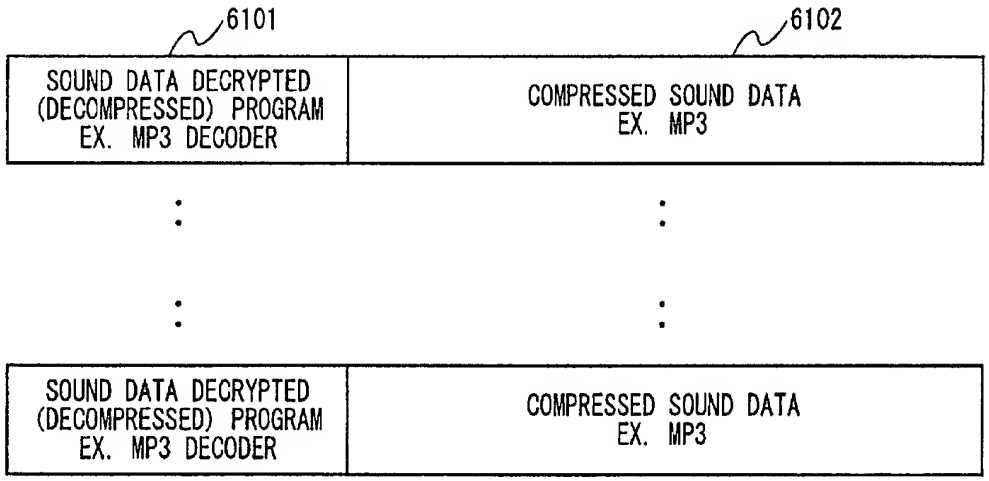


FIG. 61

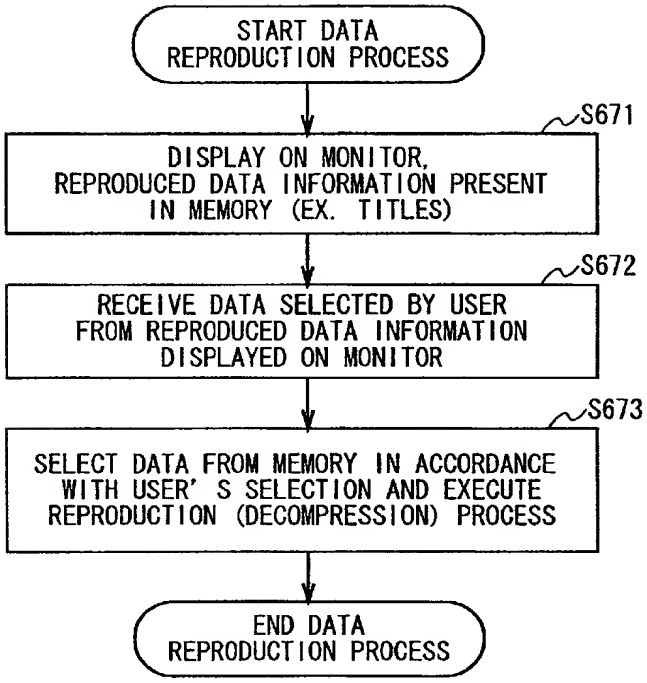

START DATA REPRODUCTION PROCESS
S671
DISPLAY ON MONITOR, REPRODUCED DATA INFORMATION PRESENT IN MEMORY (EX. TITLES)
S672
RECEIVE DATA SELECTED BY USER FROM REPRODUCED DATA INFORMATION DISPLAYED ON MONITOR
S673
SELECT DATA FROM MEMORY IN ACCORDANCE WITH USER' S SELECTION AND EXECUTE REPRODUCTION (DECOMPRESSION) PROCESS
END DATA REPRODUCTION PROCESS

FIG. 62

EXAMPLE OF CONTENT CONFIGURATION (2)

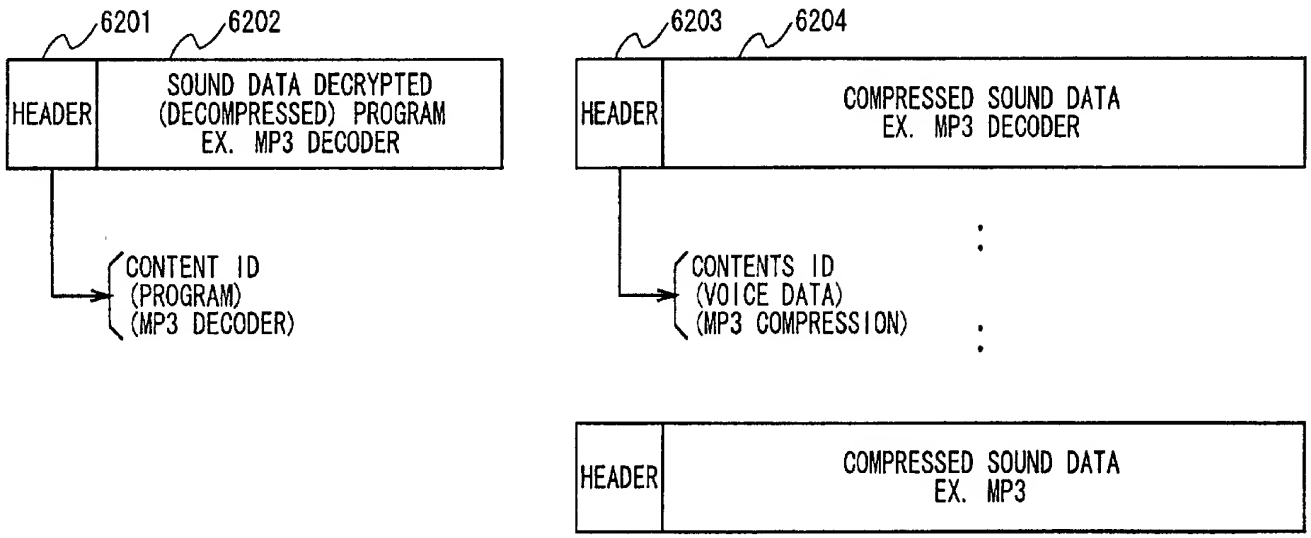


FIG. 63

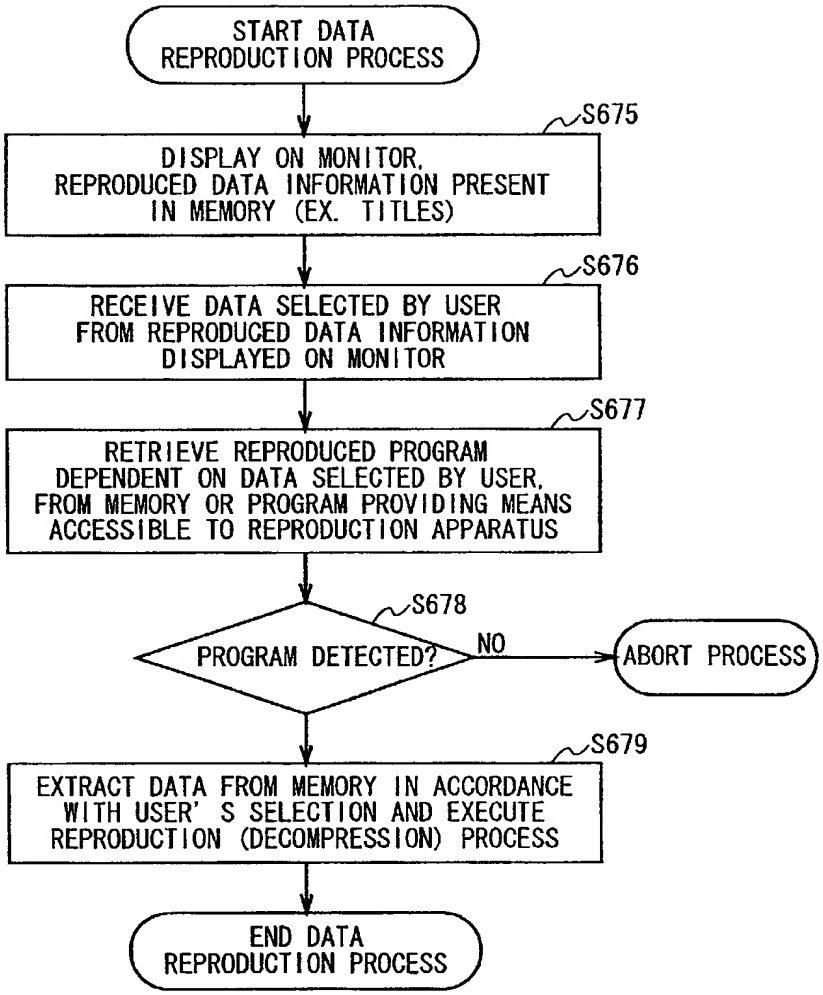

START DATA REPRODUCTION PROCESS
S675
DISPLAY ON MONITOR, REPRODUCED DATA INFORMATION PRESENT IN MEMORY (EX. TITLES)
S676
RECEIVE DATA SELECTED BY USER FROM REPRODUCED DATA INFORMATION DISPLAYED ON MONITOR
S677
RETRIEVE REPRODUCED PROGRAM DEPENDENT ON DATA SELECTED BY USER, FROM MEMORY OR PROGRAM PROVIDING MEANS ACCESSIBLE TO REPRODUCTION APPARATUS
S678
PROGRAM DETECTED?
NO
ABORT PROCESS
S679
EXTRACT DATA FROM MEMORY IN ACCORDANCE WITH USER' S SELECTION AND EXECUTE REPRODUCTION (DECOMPRESSION) PROCESS
END DATA REPRODUCTION PROCESS

FIG. 64

EXAMPLE OF CONTENT CONFIGURATION (3)

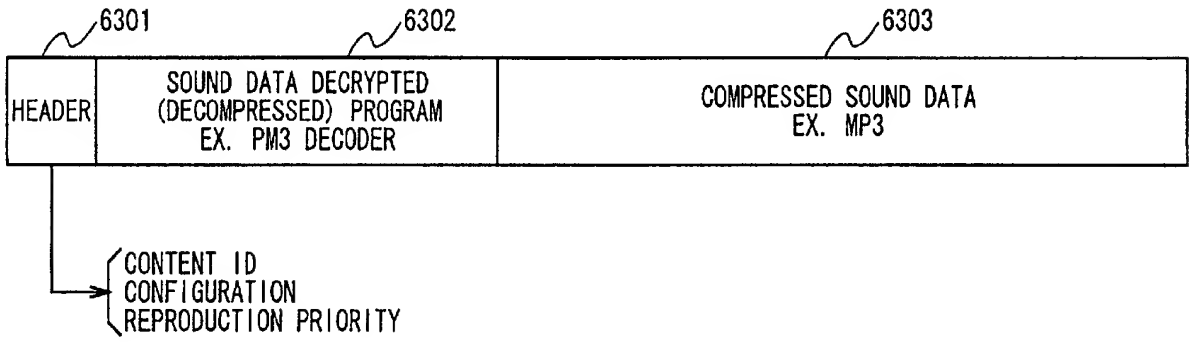


FIG. 65

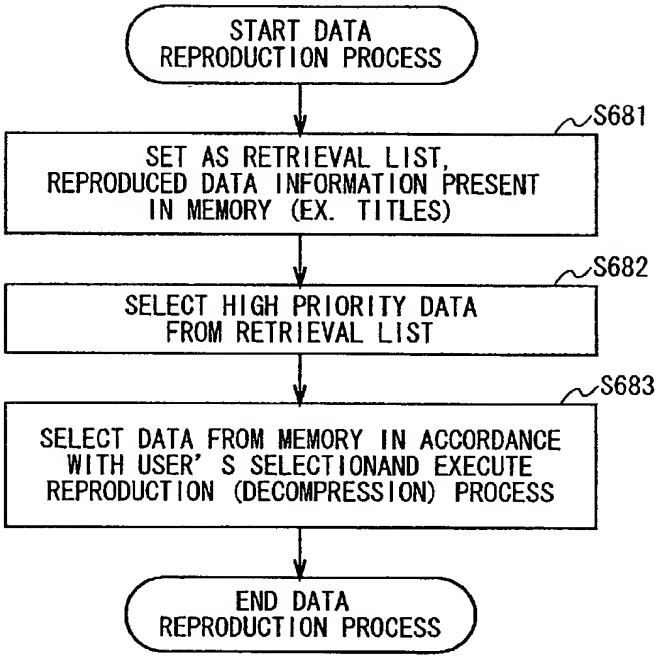

START DATA REPRODUCTION PROCESS
S681
SET AS RETRIEVAL LIST, REPRODUCED DATA INFORMATION PRESENT IN MEMORY (EX. TITLES)
S682
SELECT HIGH PRIORITY DATA FROM RETRIEVAL LIST
S683
SELECT DATA FROM MEMORY IN ACCORDANCE WITH USER' S SELECTIONAND EXECUTE REPRODUCTION (DECOMPRESSION) PROCESS
END DATA REPRODUCTION PROCESS

FIG. 66

EXAMPLE OF CONTENT CONFIGURATION (4)

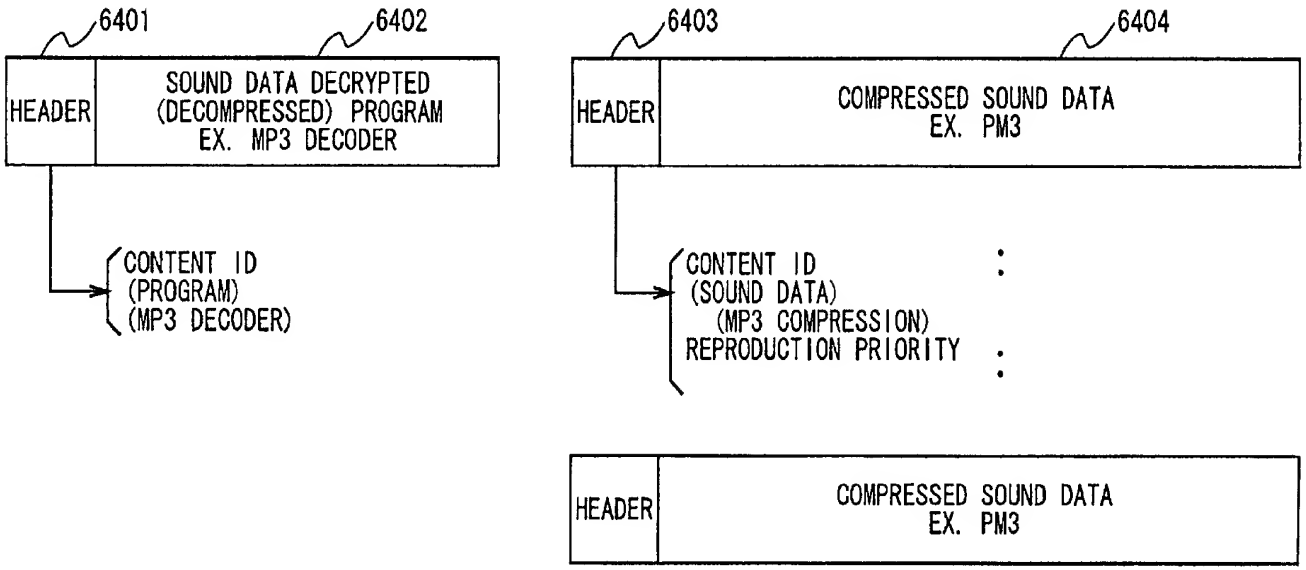


FIG. 67

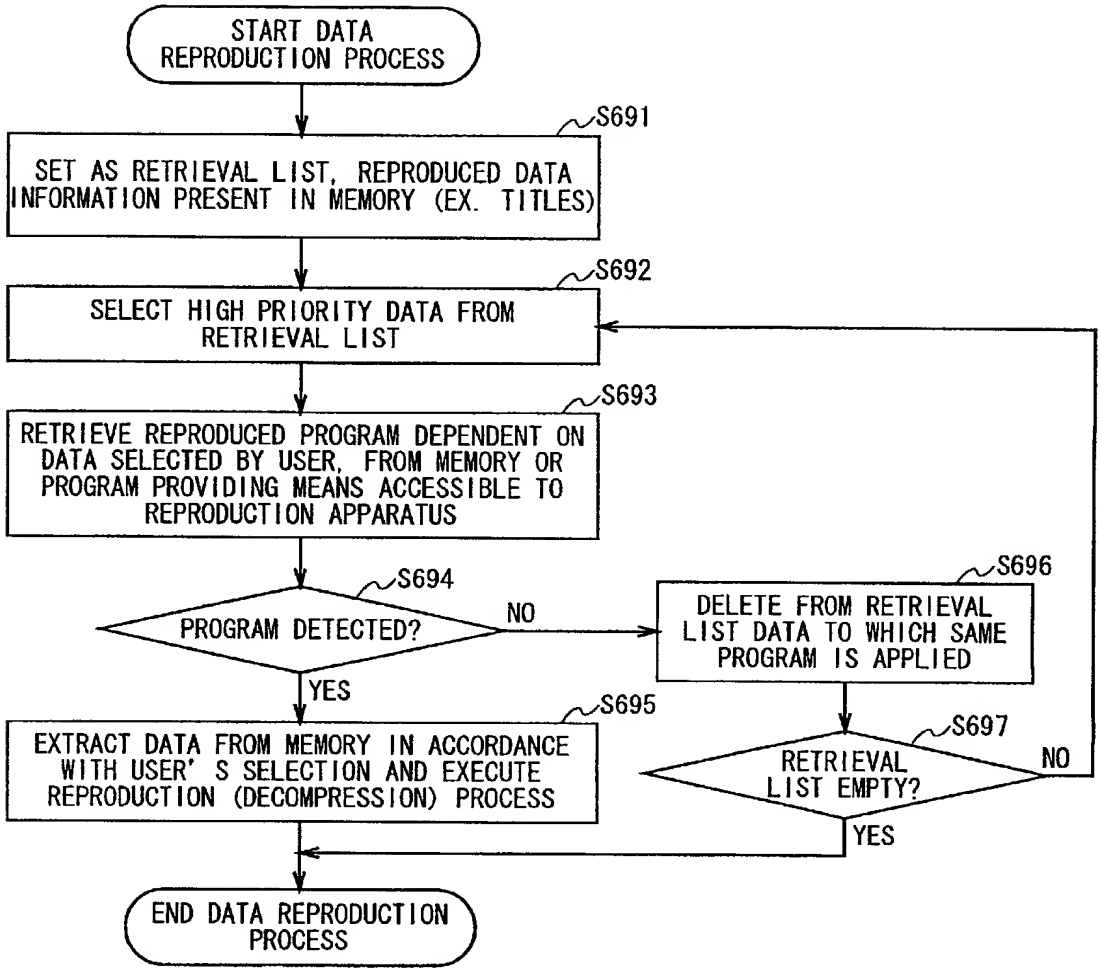
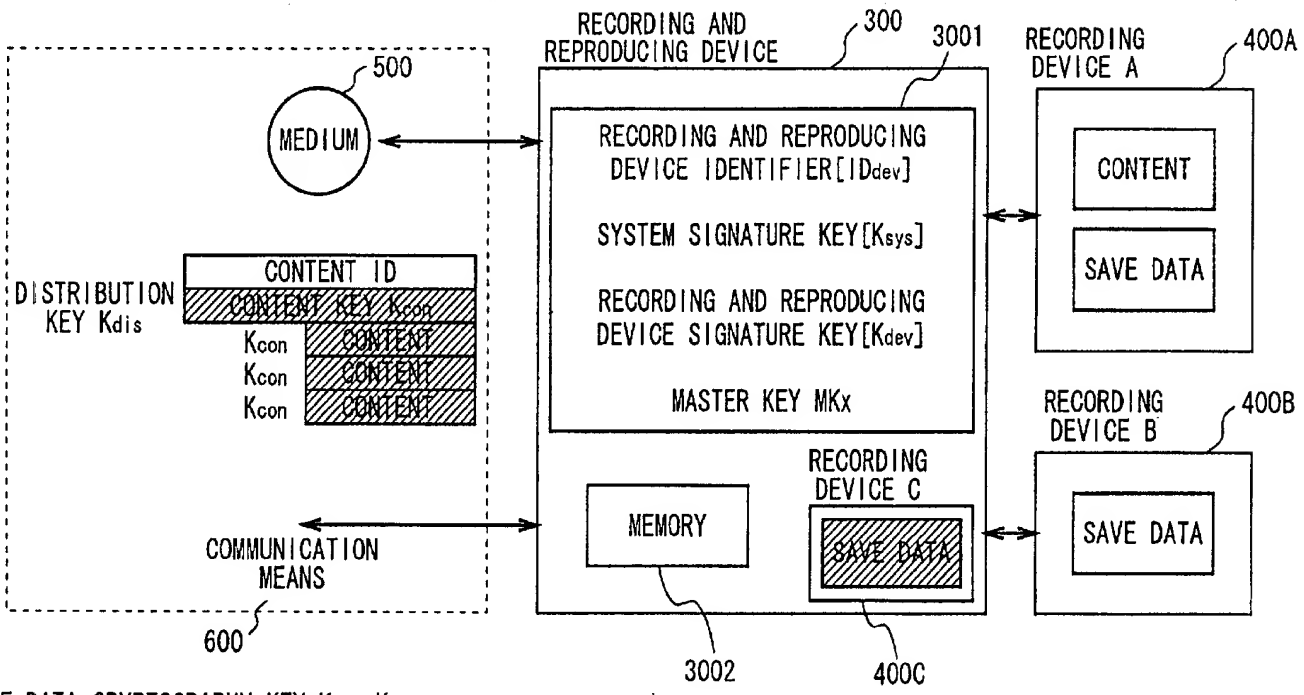

START DATA REPRODUCTION PROCESS
S691
SET AS RETRIEVAL LIST, REPRODUCED DATA INFORMATION PRESENT IN MEMORY (EX. TITLES)
S692
SELECT HIGH PRIORITY DATA FROM RETRIEVAL LIST
S693
RETRIEVE REPRODUCED PROGRAM DEPENDENT ON DATA SELECTED BY USER, FROM MEMORY OR PROGRAM PROVIDING MEANS ACCESSIBLE TO REPRODUCTION APPARATUS
S694
PROGRAM DETECTED?
NO
S696
DELETE FROM RETRIEVAL LIST DATA TO WHICH SAME PROGRAM IS APPLIED
YES
S695
EXTRACT DATA FROM MEMORY IN ACCORDANCE WITH USER' S SELECTION AND EXECUTE REPRODUCTION (DECOMPRESSION) PROCESS
S697
RETRIEVAL LIST EMPTY?
NO
YES
END DATA REPRODUCTION PROCESS

FIG. 68



SAVE DATA CRYPTOGRAPHY KEY:$K_{sav}=K_{con}$
SAVE DATA CRYPTOGRAPHY KEY:$K_{sav}=K_{sys}$
SAVE DATA CRYPTOGRAPHY KEY:$K_{sav}=K_{dev}$
SAVE DATA CRYPTOGRAPHY KEY:K_{sav}=CONTENT ID OR DES (MKx, CONTENT ID)
SAVE DATA CRYPTOGRAPHY KEY:K_{sav}=RECORDING AND REPRODUCING DEVICE ID(ID_{dev}) or DES (MKx, RECORDING AND REPRODUCING DEVICE ID(ID_{dev}))
SAVE DATA CRYPTOGRAPHY KEY:$K_{sav}=(K_{con} \hat{} K_{dev})$ or DES(MK_x, $K_{con} \hat{} K_{dev}$)
SAVE DATA CRYPTOGRAPHY KEY:K_{sav}=(CONTENT ID$\hat{}K_{dev}$) or DES(MK_x, CONTENT ID$\hat{}K_{dev}$)
SAVE DATA CRYPTOGRAPHY KEY:K_{sav}=(KCON^RECORDING AND REPRODUCING DEVICE ID) OR DES (MKx, KCON^RECORDING AND REPRODUCING DEVICE ID)
SAVE DATA CRYPTOGRAPHY KEY:K_{sav}=(CONTENT ID^RECORDING AND REPRODUCING DEVICE ID) OR DES (MKX, CONTENT ID^RECORDING AND REPRODUCING DEVICE ID)
SAVE DATA CRYPTOGRAPHY KEY:K_{sav}=PASSWORD OR DES(MKX, PASSWORD) ETC.

FIG. 69

(1) EXAMPLE OF SAVE DATA STORAGE PROCESS USING CONTENT UNIQUE KEY CONTENT OR SYSTEM COMMON KEY

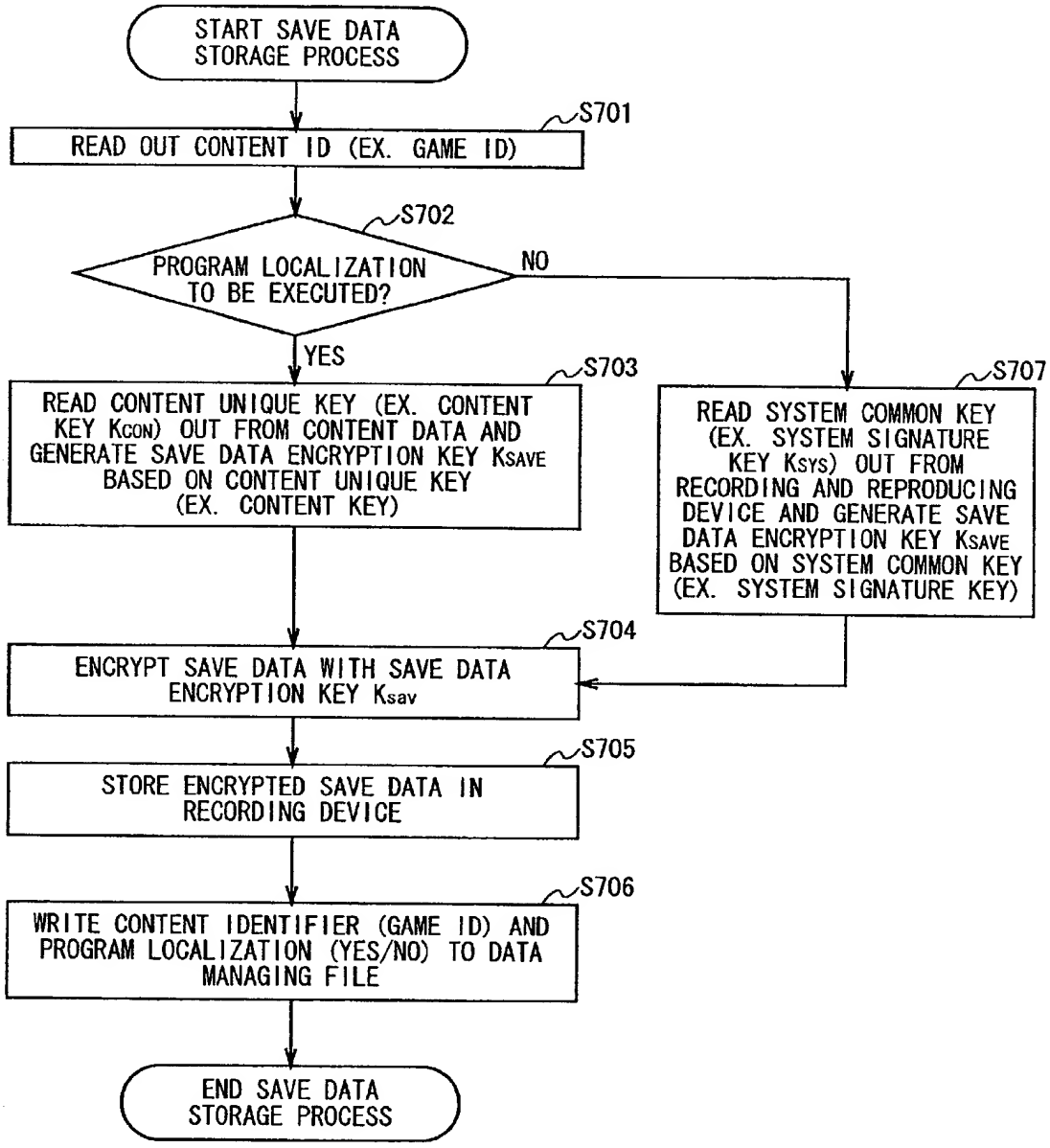


FIG. 70

DATA MANAGING FILE(1)

DATA NUMBER	CONTENT ID (GAME ID)	RECORDING AND REPRODUCING DEVICE ID (IDDEV)	PROGRAM LOCALIZATION
1	12345678...	56789012...	YES
2	ABCDEF12...	09876543...	YES
3	12245678...	58834762...	NO
:	:	:	:

FIG. 71

(2) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING CONTENT UNIQUE KEY OR SYSTEM COMMON KEY

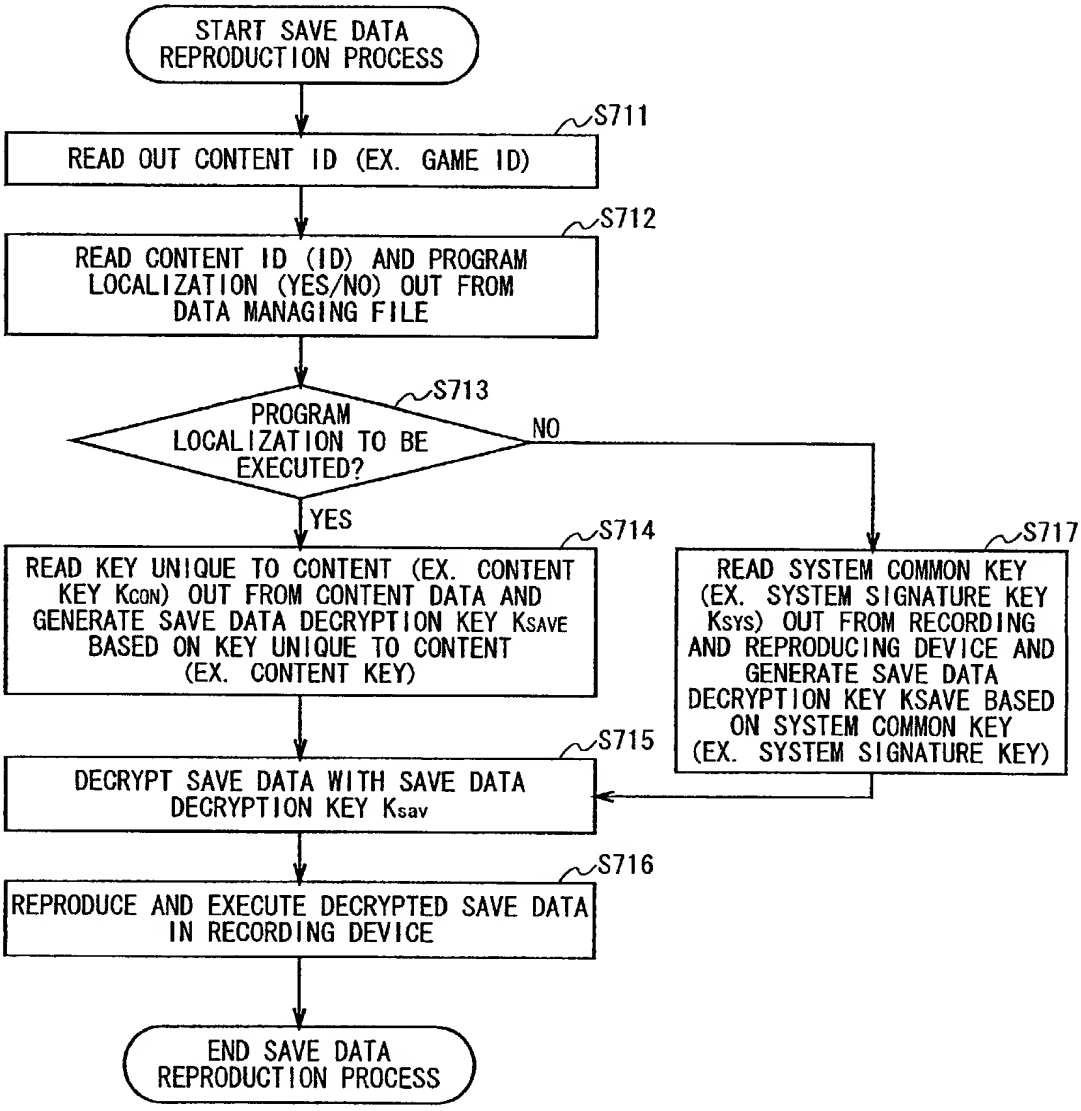


FIG. 72

(3) EXAMPLE OF SAVE DATA STORAGE PROCESS USING CONTENT ID OR SYSTEM COMMON KEY

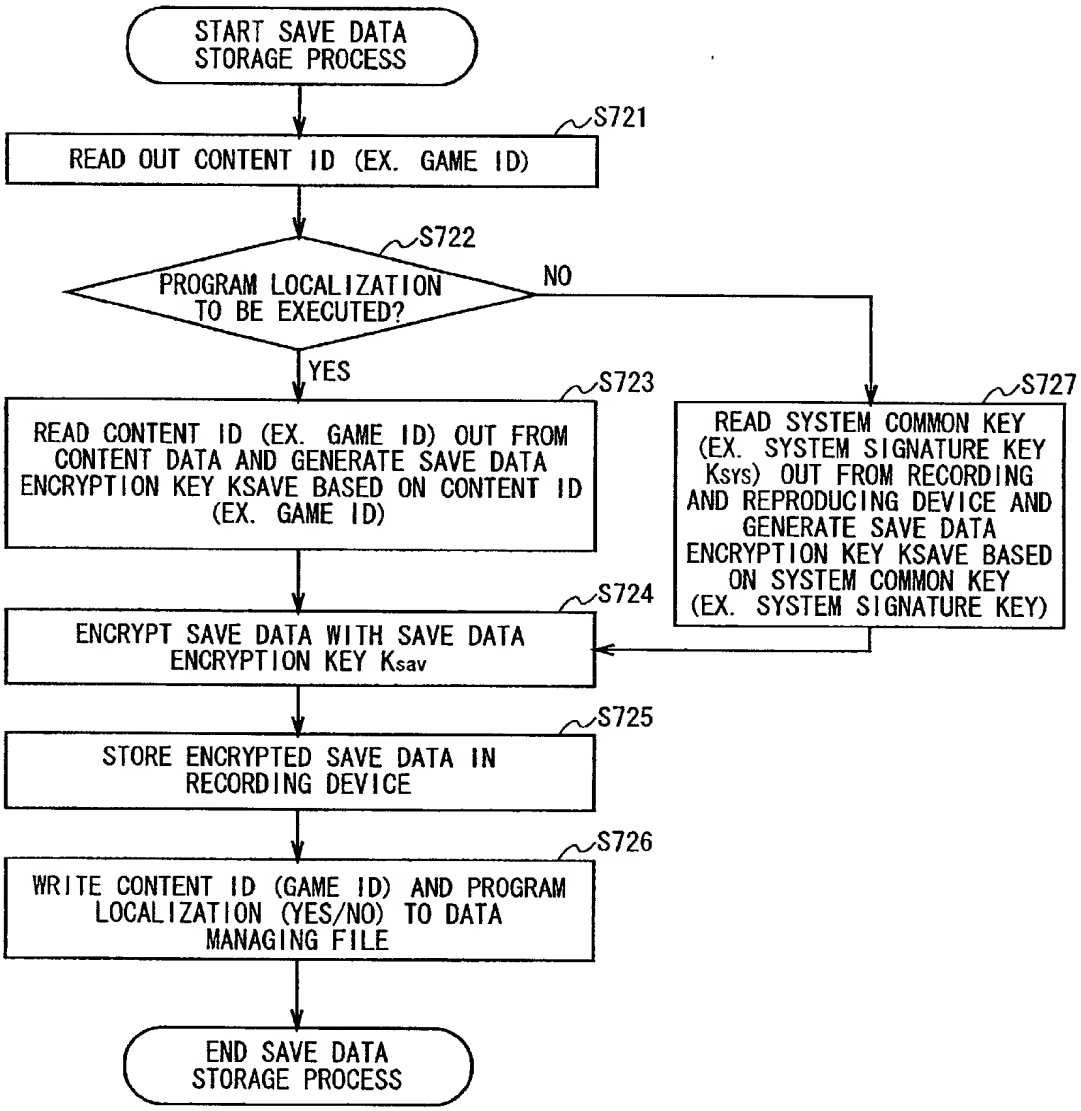


FIG. 73

(4) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING CONTENT ID OR SYSTEM COMMON KEY

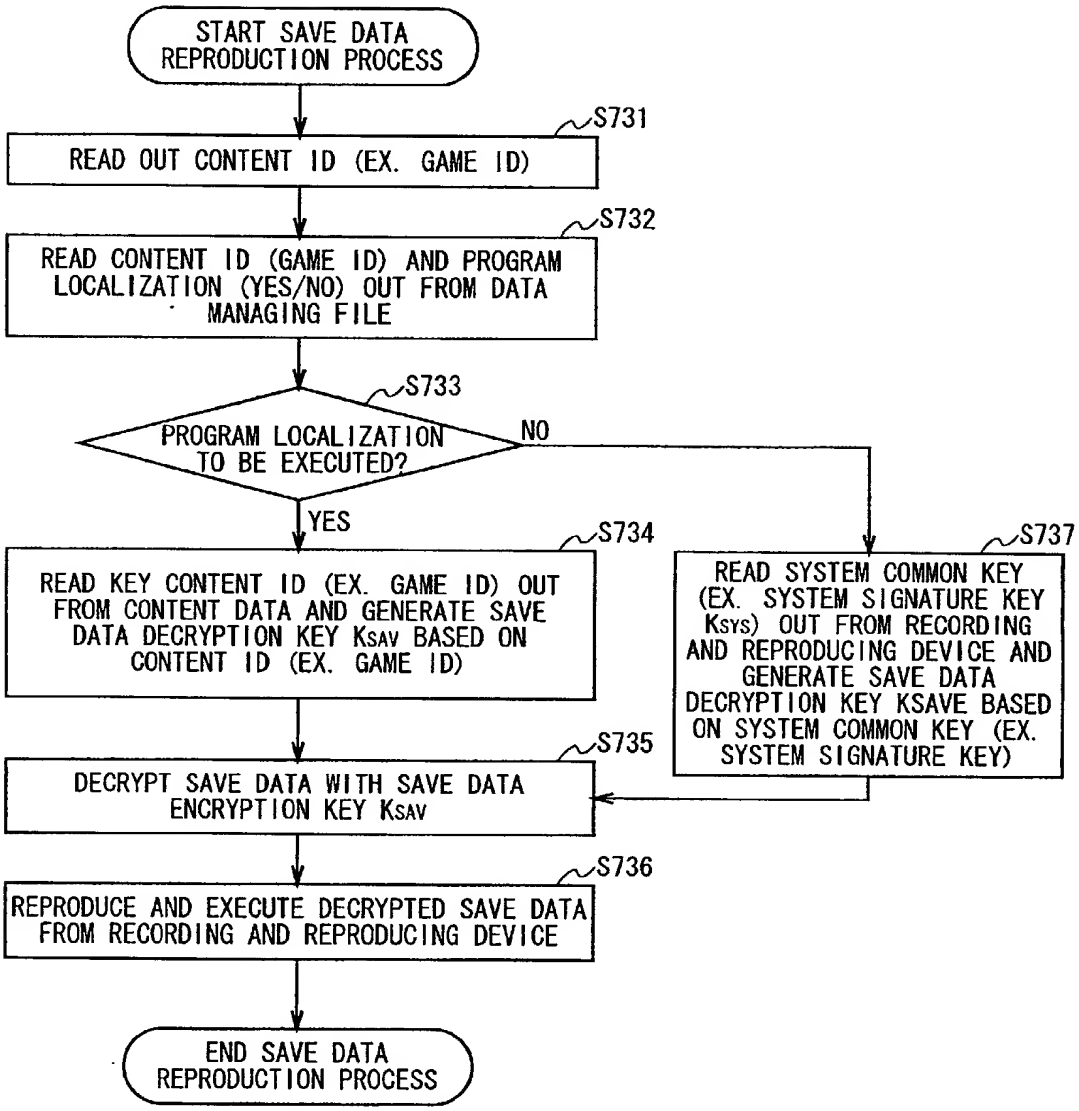


FIG. 74

(5) EXAMPLE OF SAVE DATA STORAGE PROCESS USING RECORDING AND REPRODUCING DEVICE UNIQUE KEY OR SYSTEM COMMON KEY

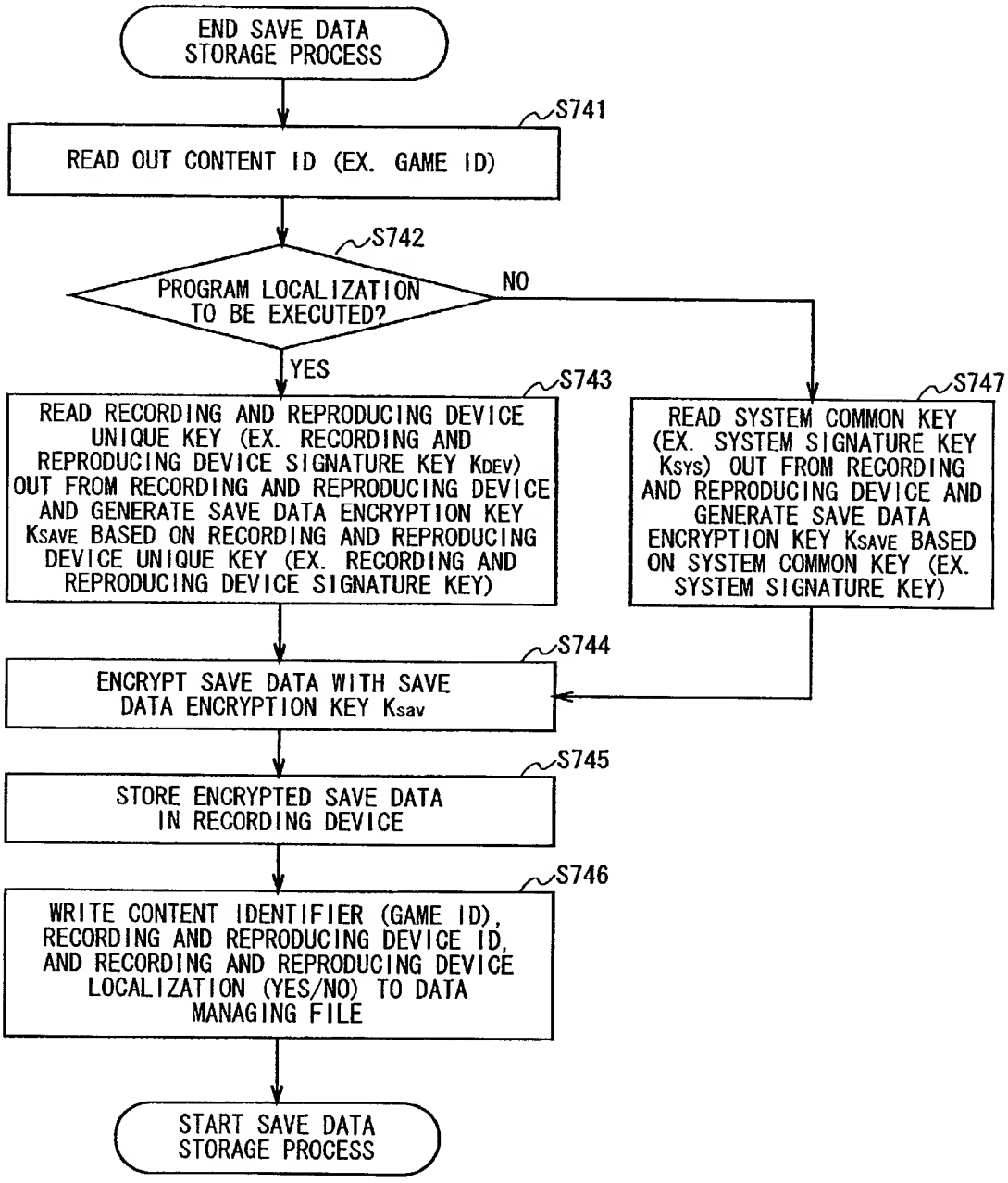


FIG. 75

DATA MANAGING FILE(2)

DATA NUMBER	CONTENT ID (GAME ID)	RECORDING AND REPRODUCING DEVICE ID (IDdev)	PROGRAM LOCALIZATION
1	12345678...	56789012...	NO
2	ABCDEF12...	09876543...	YES
3	12245678...	58834762...	YES
:	:	:	:

FIG. 76

(6) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING RECORDING AND REPRODUCING DEVICE UNIQUE KEY OR SYSTEM COMMON KEY

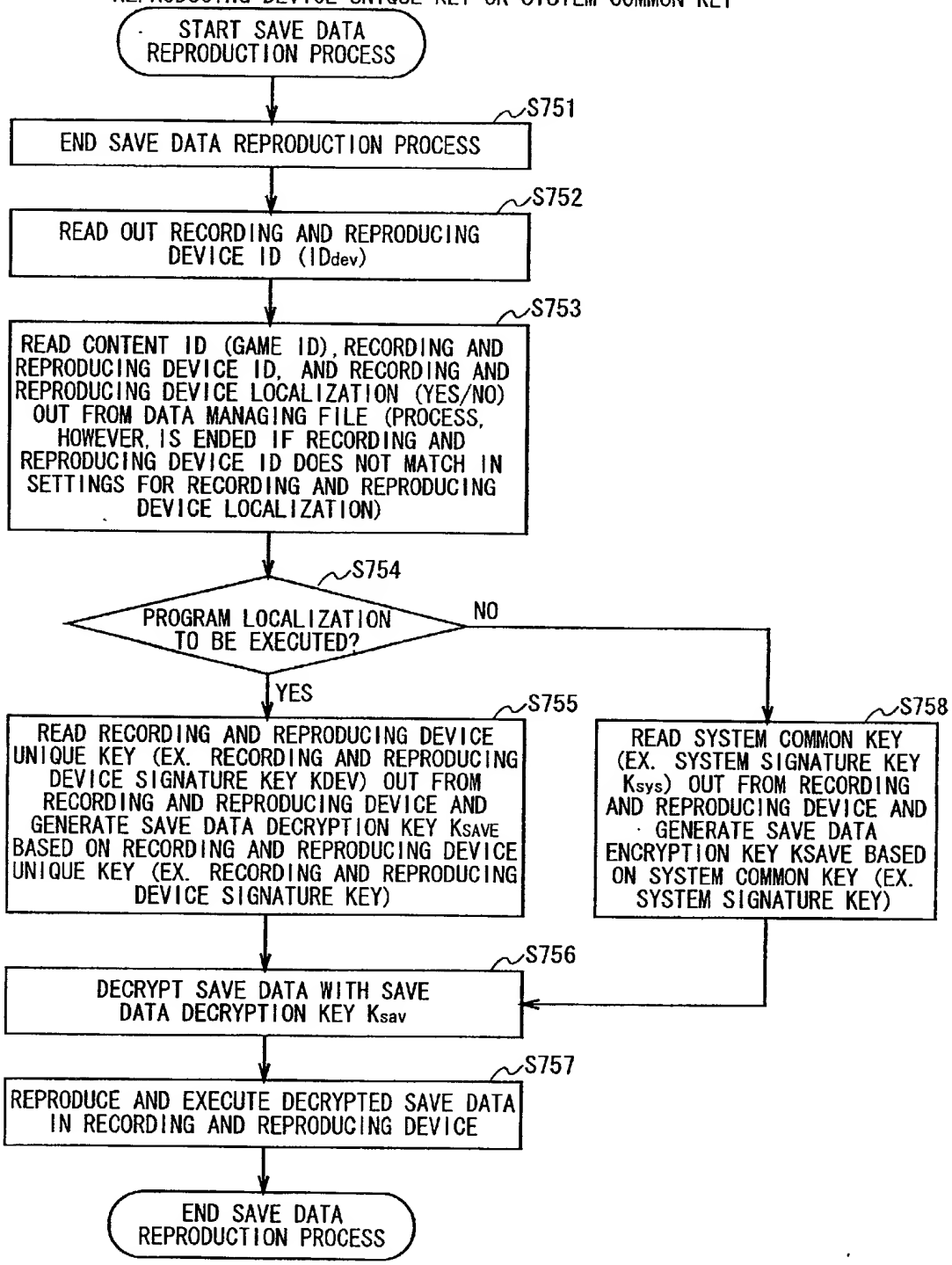


FIG. 77

(7) EXAMPLE OF SAVE DATA STORAGE PROCESS USING RECORDING AND REPRODUCING DEVICE ID OR SYSTEM COMMON KEY

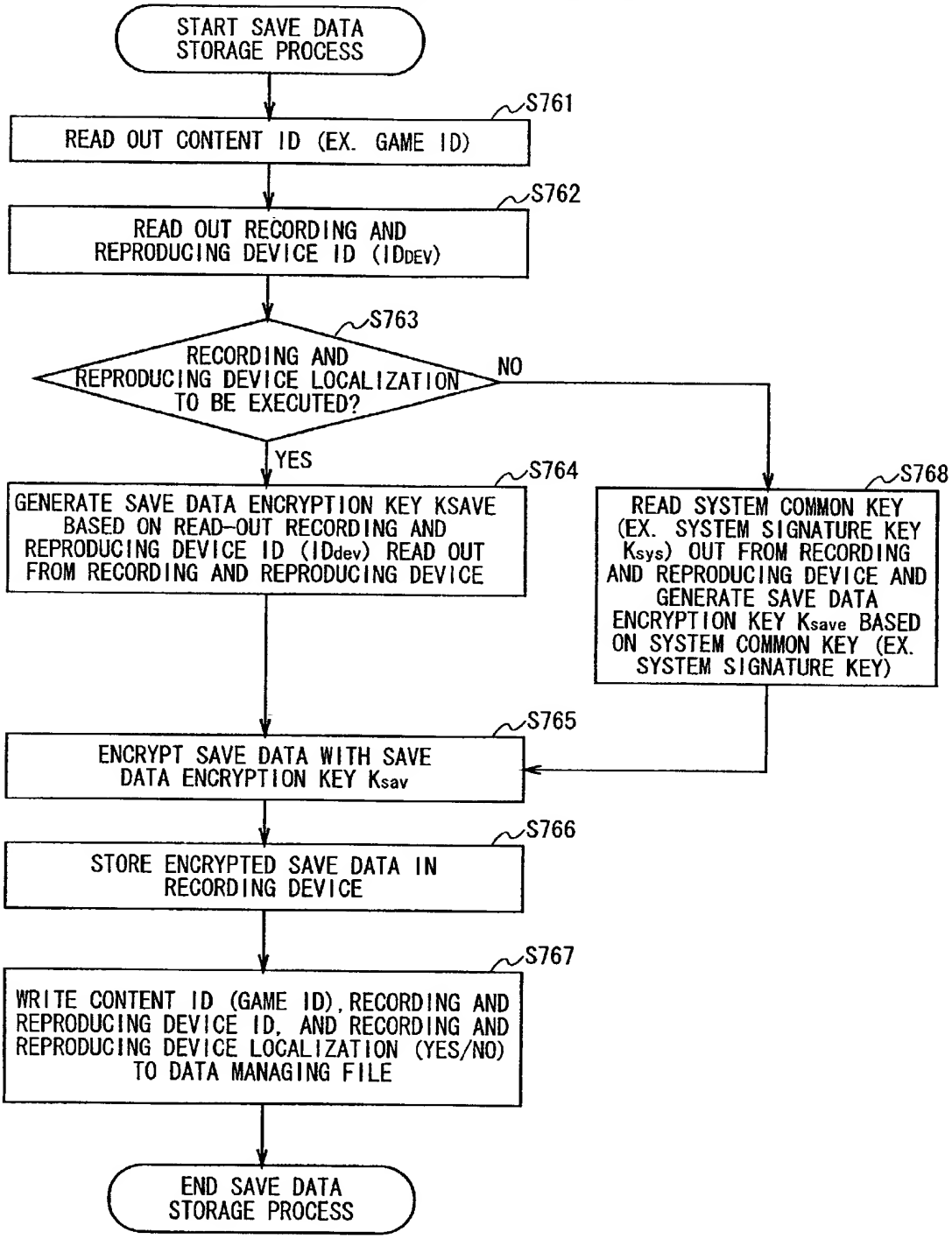


FIG. 78

(8) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING RECORDING AND REPRODUCING DEVICE ID OR SYSTEM COMMON KEY

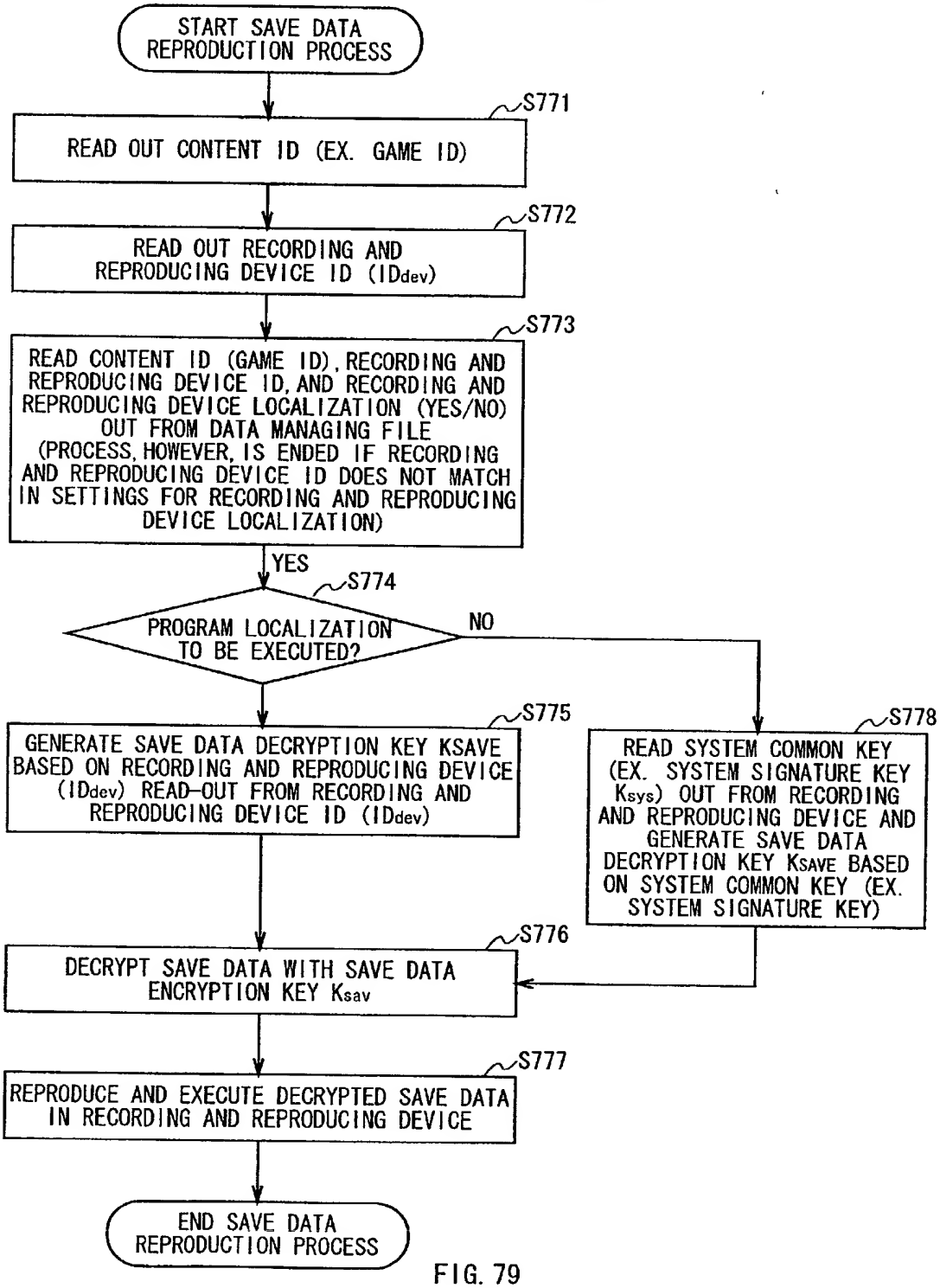


FIG. 79

(9) EXAMPLE OF SAVE DATA STORAGE PROCESS USING CONTENT UNIQUE KEY, RECORDING AND REPRODUCING DEVICE UNIQUE KEY, OR SYSTEM COMMON KEY

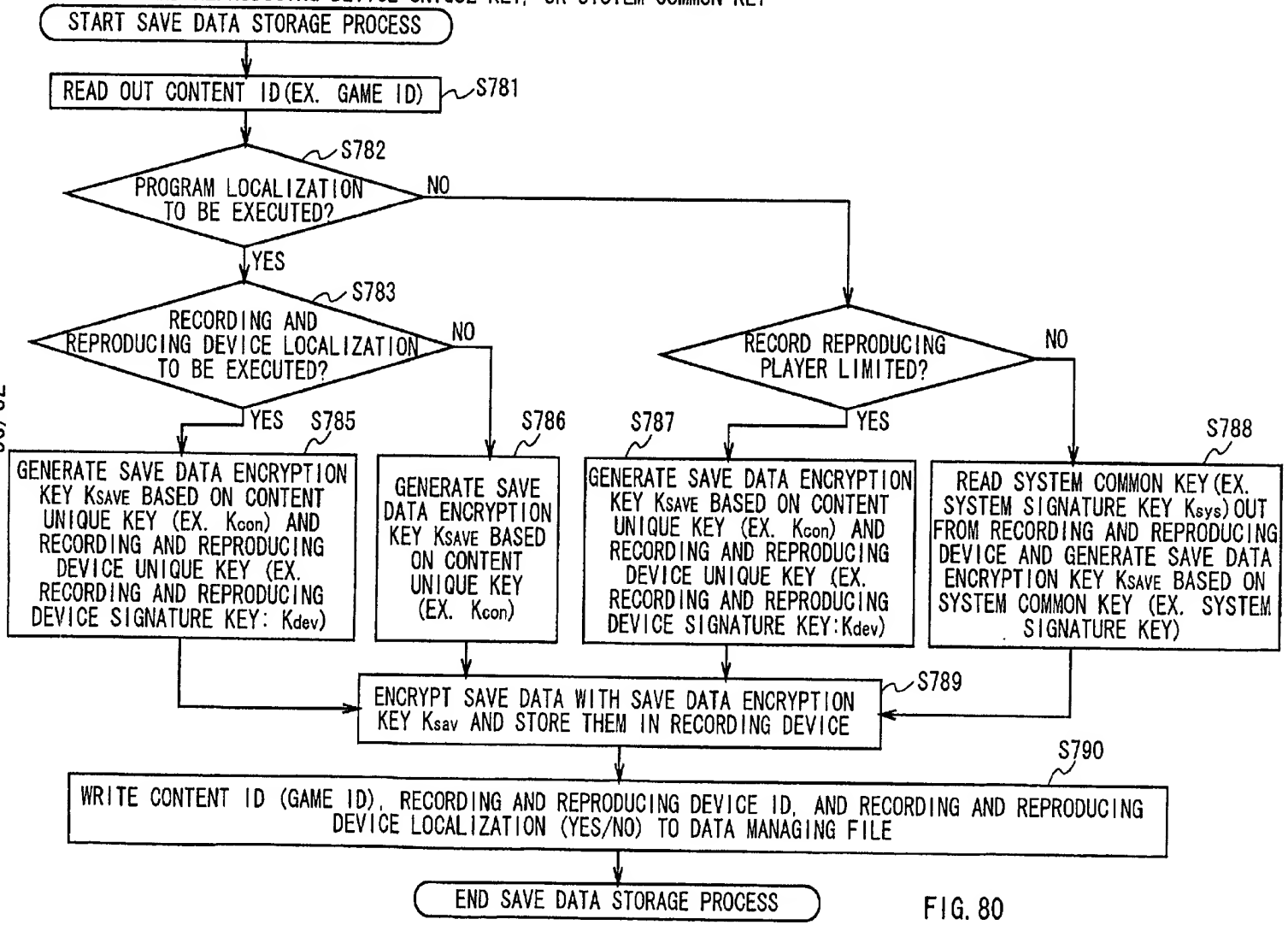


FIG. 80

DATA MANAGING FILE(3)

DATA NUMBER	CONTENT ID (GAME ID)	RECORDING AND REPRODUCING DEVICE ID (ID_{dev})	PROGRAM LOCALIZATION	RECORDING AND REPRODUCING DEVICE LOCALIZATION
1	123455678...	56789012...	YES	NO
2	ABCDEF12...	09876543...	YES	YES
3	1122457678	58834762...	NO	YES
⋮	⋮	⋮	⋮	⋮

FIG. 81

(10) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING CONTENT UNIQUE KEY, RECORDING AND REPRODUCING DEVICE UNIQUE KEY, OR SYSTEM COMMON KEY

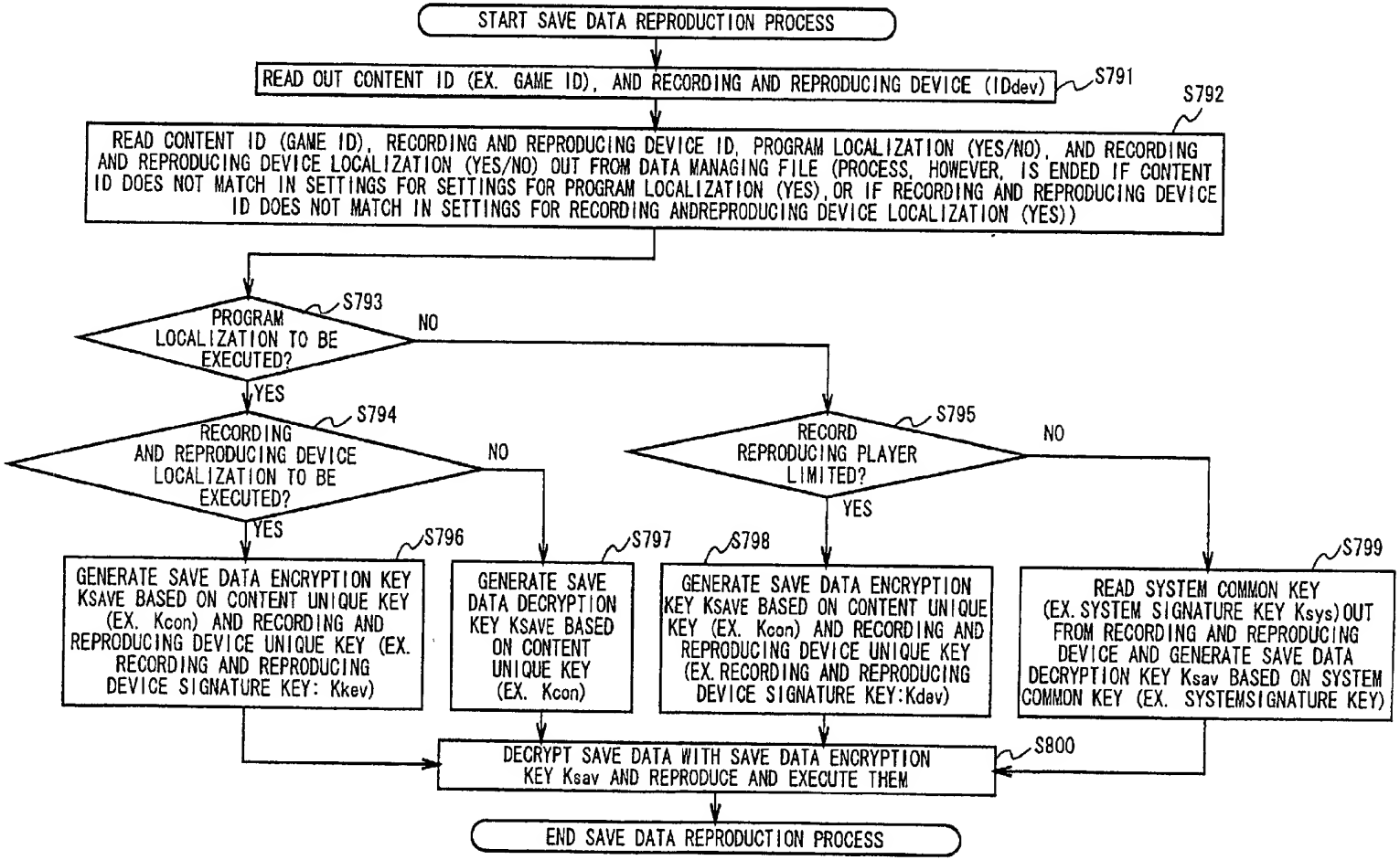


FIG. 82

(11) EXAMPLE OF SAVE DATA STORAGE PROCESS USING USER PASSWORD OR SYSTEM COMMON KEY

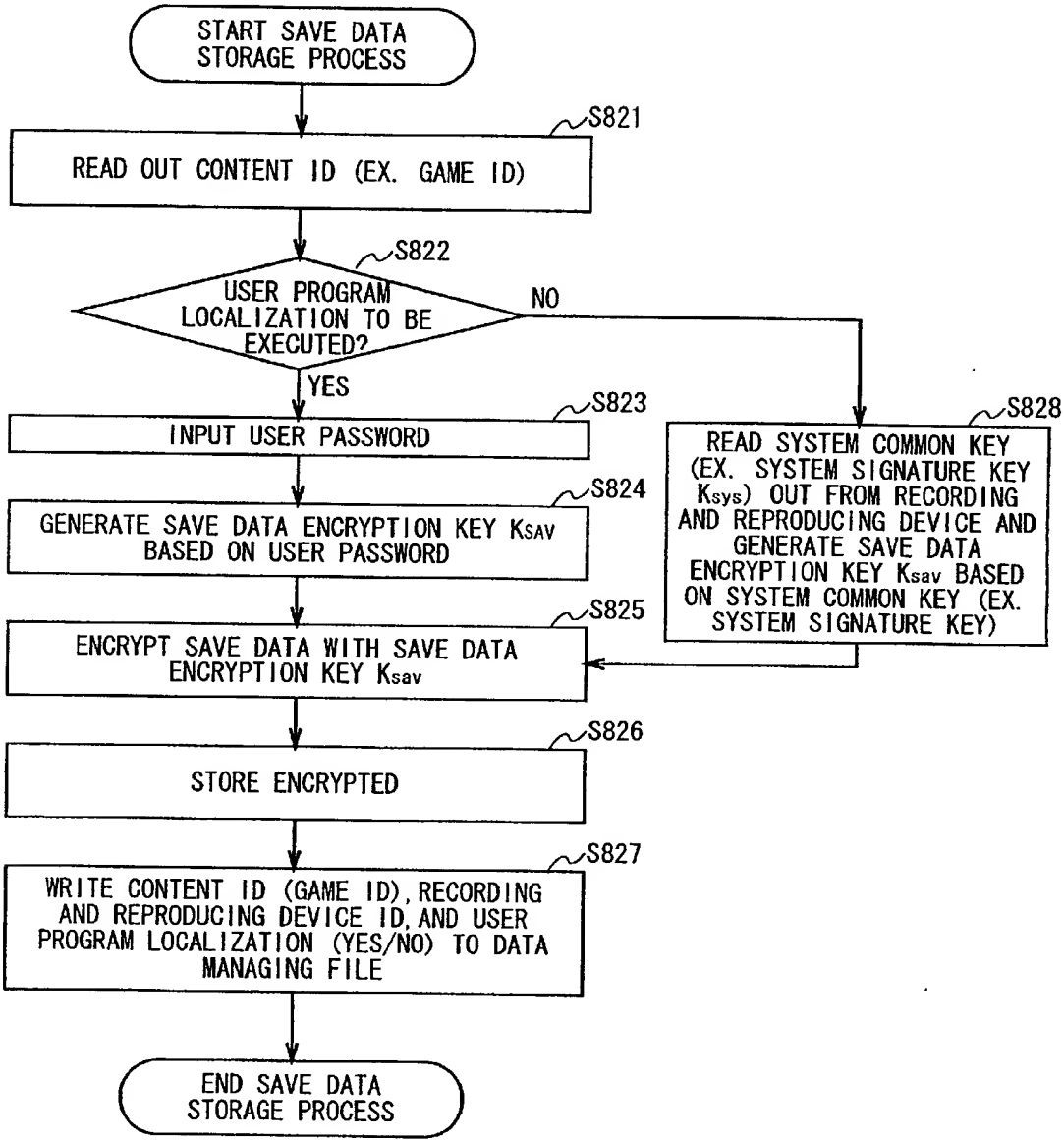


FIG. 83

DATA MANAGING FILE(4)

DATA NUMBER	CONTENT ID (GAME ID)	RECORDING AND REPRODUCING DEVICE ID (ID_{dev})	USER PROGRAM LOCALIZATION
1	123455678...	56789012...	YES
2	ABCDEF12...	09876543...	YES
3	1122457678	58834762...	NO
⋮	⋮	⋮	⋮

FIG. 84

(12) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING USER PASSWORD OR SYSTEM COMMON KEY

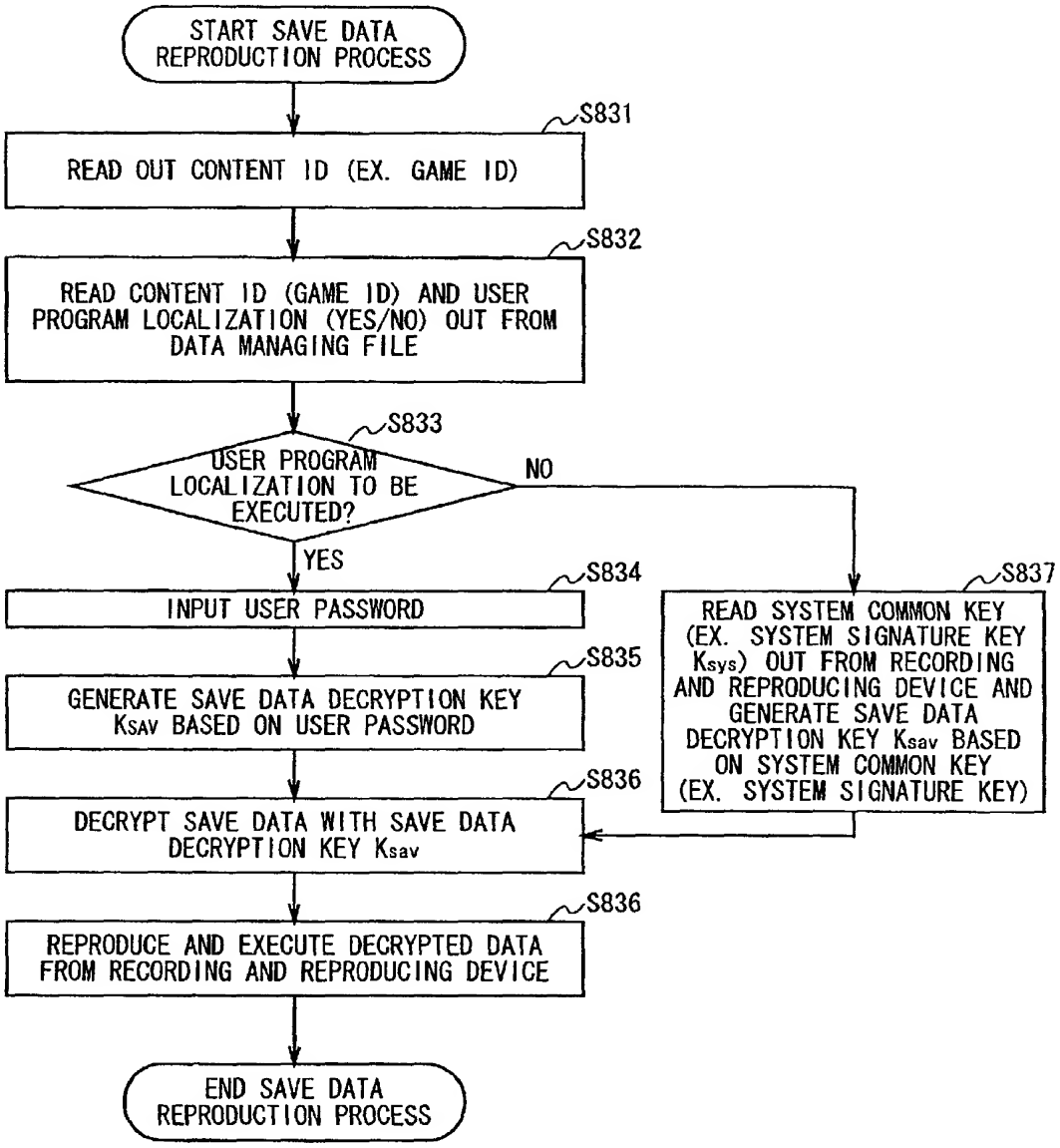


FIG. 85

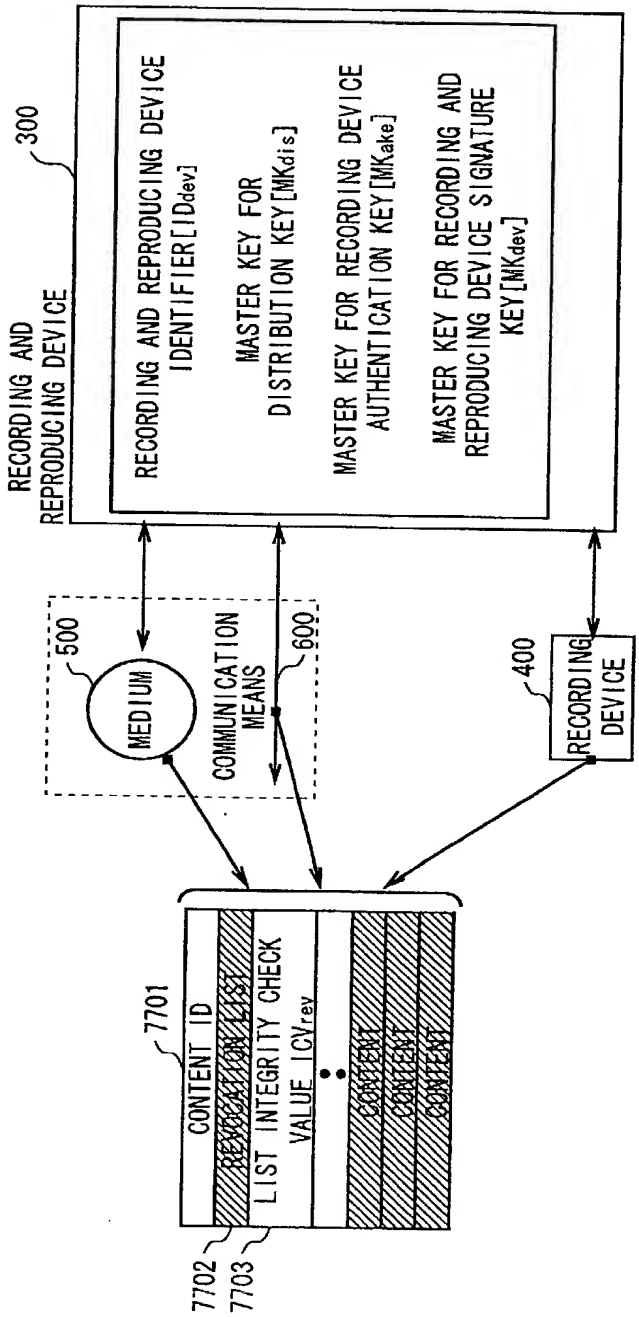

RECORDING AND REPRODUCING DEVICE
300
RECORDING AND REPRODUCING DEVICE IDENTIFIER[IDdev]
MASTER KEY FOR DISTRIBUTION KEY[MKdis]
MASTER KEY FOR RECORDING DEVICE AUTHENTICATION KEY[MKake]
MASTER KEY FOR RECORDING AND REPRODUCING DEVICE SIGNATURE KEY[MKdev]
500
MEDIUM
COMMUNICATION MEANS
600
400
RECORDING DEVICE
7701
CONTENT ID
REVOCATION LIST
LIST INTEGRITY CHECK VALUE ICVrev
CONTENT
CONTENT
CONTENT
7702
7703

FIG. 86

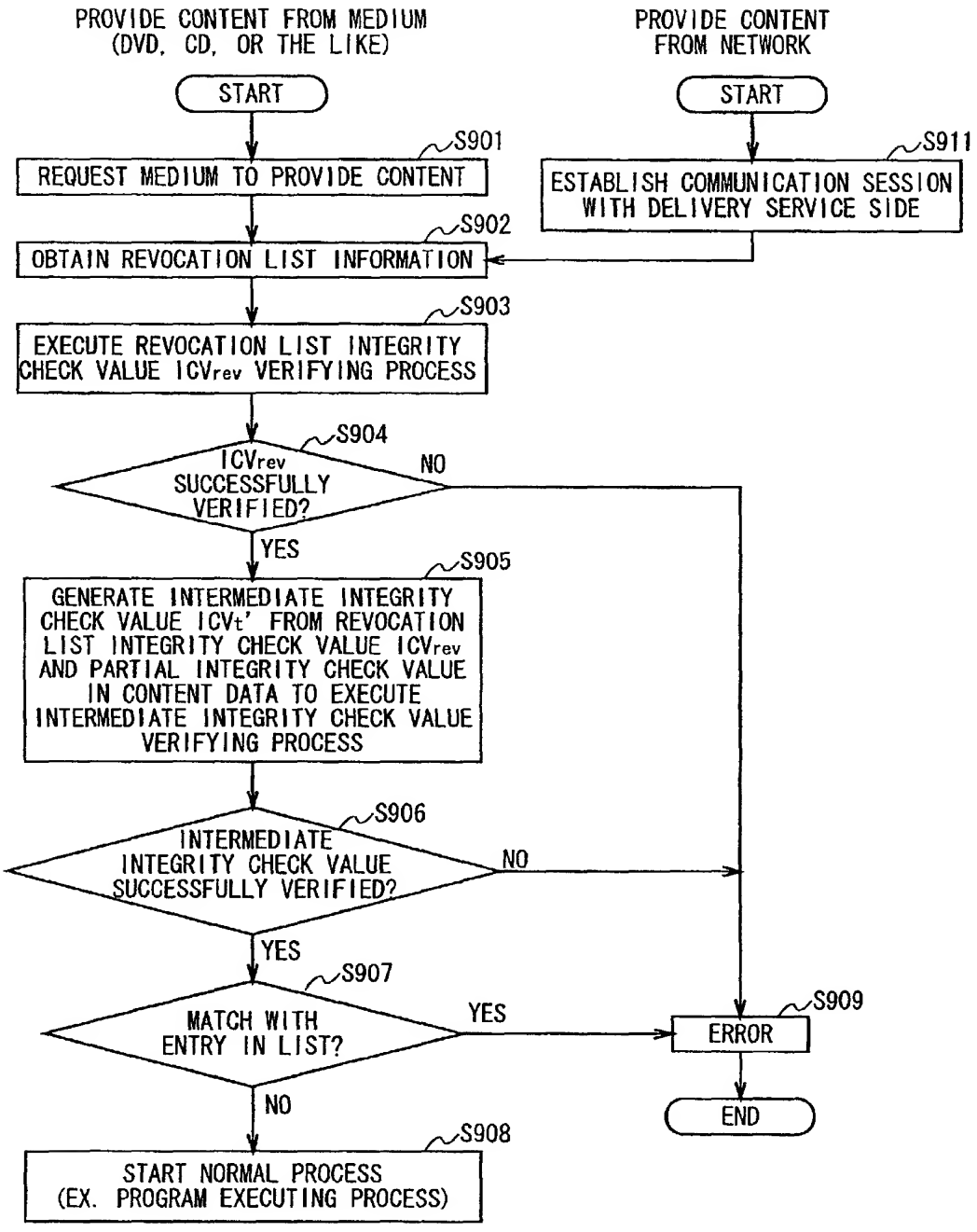

PROVIDE CONTENT FROM MEDIUM (DVD, CD, OR THE LIKE)
PROVIDE CONTENT FROM NETWORK
START
START
S901
REQUEST MEDIUM TO PROVIDE CONTENT
S911
ESTABLISH COMMUNICATION SESSION WITH DELIVERY SERVICE SIDE
S902
OBTAIN REVOCATION LIST INFORMATION
S903
EXECUTE REVOCATION LIST INTEGRITY CHECK VALUE ICVrev VERIFYING PROCESS
S904
ICVrev SUCCESSFULLY VERIFIED?
NO
YES
S905
GENERATE INTERMEDIATE INTEGRITY CHECK VALUE ICVt' FROM REVOCATION LIST INTEGRITY CHECK VALUE ICVrev AND PARTIAL INTEGRITY CHECK VALUE IN CONTENT DATA TO EXECUTE INTERMEDIATE INTEGRITY CHECK VALUE VERIFYING PROCESS
S906
INTERMEDIATE INTEGRITY CHECK VALUE SUCCESSFULLY VERIFIED?
NO
YES
S907
MATCH WITH ENTRY IN LIST?
YES
S909
ERROR
NO
END
S908
START NORMAL PROCESS (EX. PROGRAM EXECUTING PROCESS)

FIG. 87

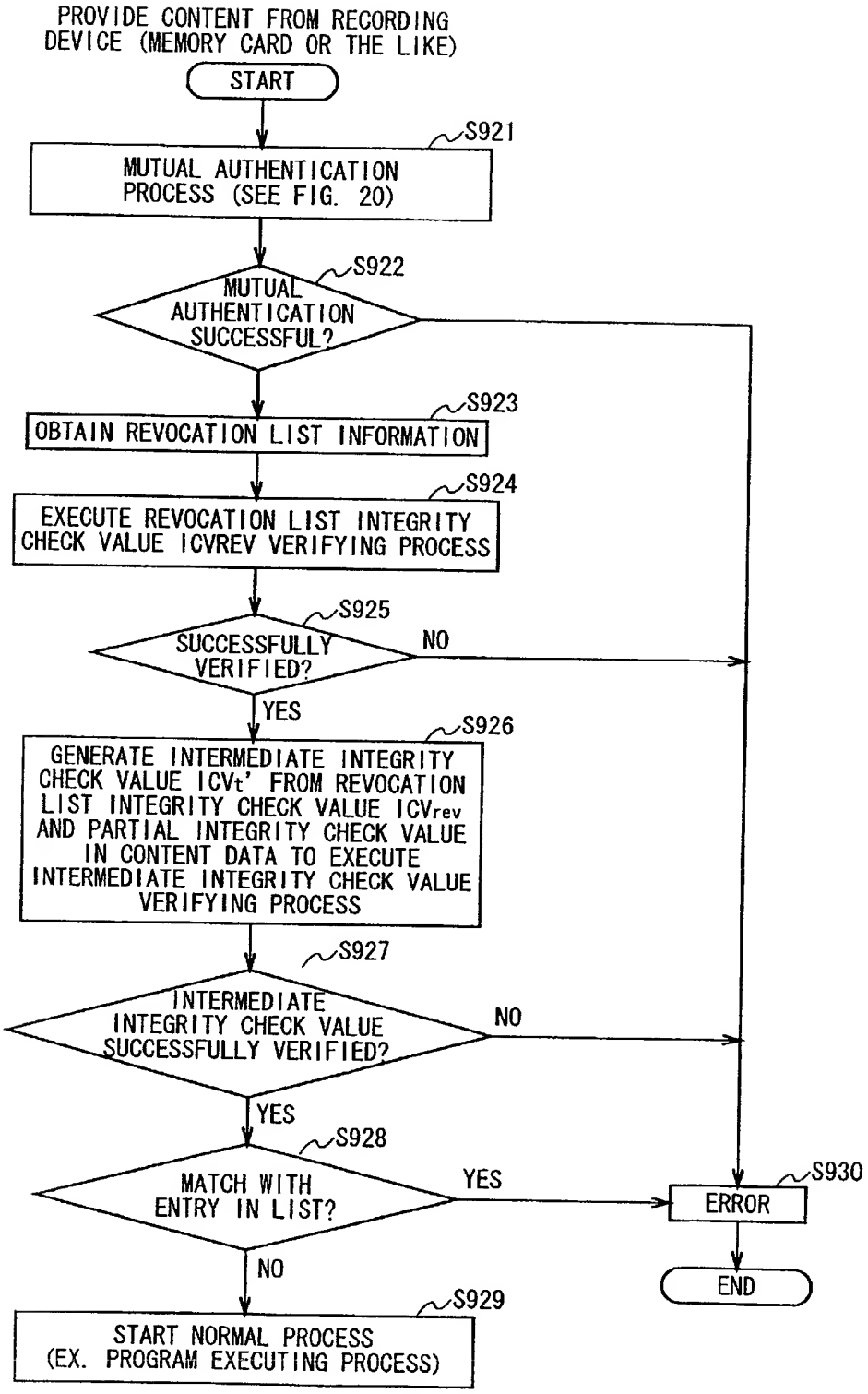

PROVIDE CONTENT FROM RECORDING DEVICE (MEMORY CARD OR THE LIKE)
START
S921
MUTUAL AUTHENTICATION PROCESS (SEE FIG. 20)
S922
MUTUAL AUTHENTICATION SUCCESSFUL?
S923
OBTAIN REVOCATION LIST INFORMATION
S924
EXECUTE REVOCATION LIST INTEGRITY CHECK VALUE ICVREV VERIFYING PROCESS
S925
SUCCESSFULLY VERIFIED?
NO
YES
S926
GENERATE INTERMEDIATE INTEGRITY CHECK VALUE ICVt' FROM REVOCATION LIST INTEGRITY CHECK VALUE ICVrev AND PARTIAL INTEGRITY CHECK VALUE IN CONTENT DATA TO EXECUTE INTERMEDIATE INTEGRITY CHECK VALUE VERIFYING PROCESS
S927
INTERMEDIATE INTEGRITY CHECK VALUE SUCCESSFULLY VERIFIED?
NO
YES
S928
MATCH WITH ENTRY IN LIST?
YES
S930
ERROR
END
NO
S929
START NORMAL PROCESS (EX. PROGRAM EXECUTING PROCESS)

FIG. 88

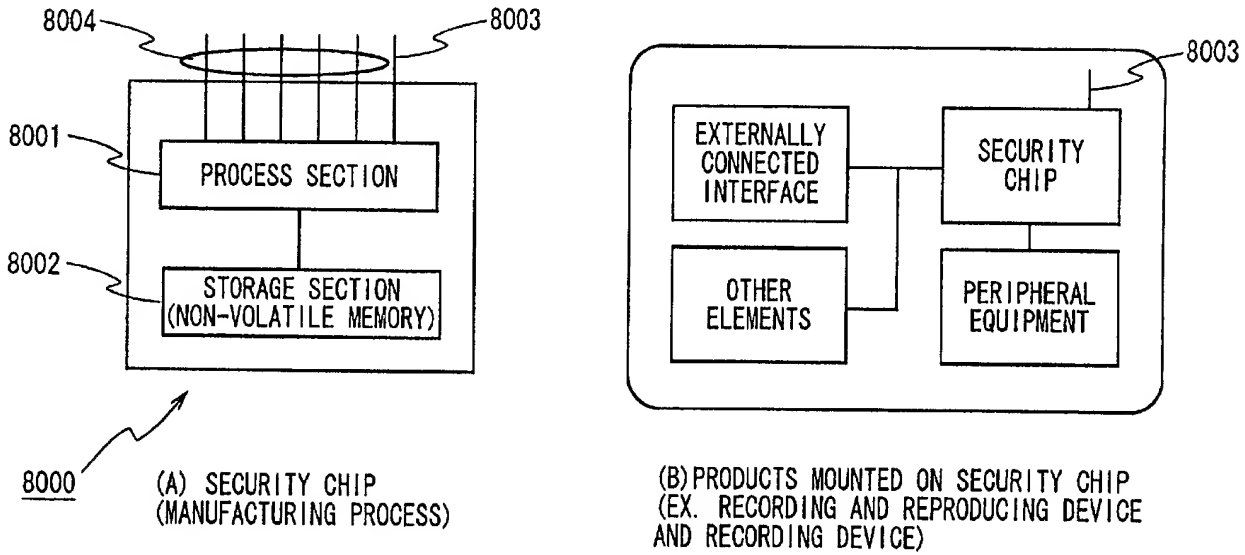

8004
8003
8001
PROCESS SECTION
8002
STORAGE SECTION
(NON-VOLATILE MEMORY)
8000
(A) SECURITY CHIP
(MANUFACTURING PROCESS)
8003
EXTERNALLY
CONNECTED
INTERFACE
SECURITY
CHIP
OTHER
ELEMENTS
PERIPHERAL
EQUIPMENT
(B) PRODUCTS MOUNTED ON SECURITY CHIP
(EX. RECORDING AND REPRODUCING DEVICE
AND RECORDING DEVICE)

FIG. 89

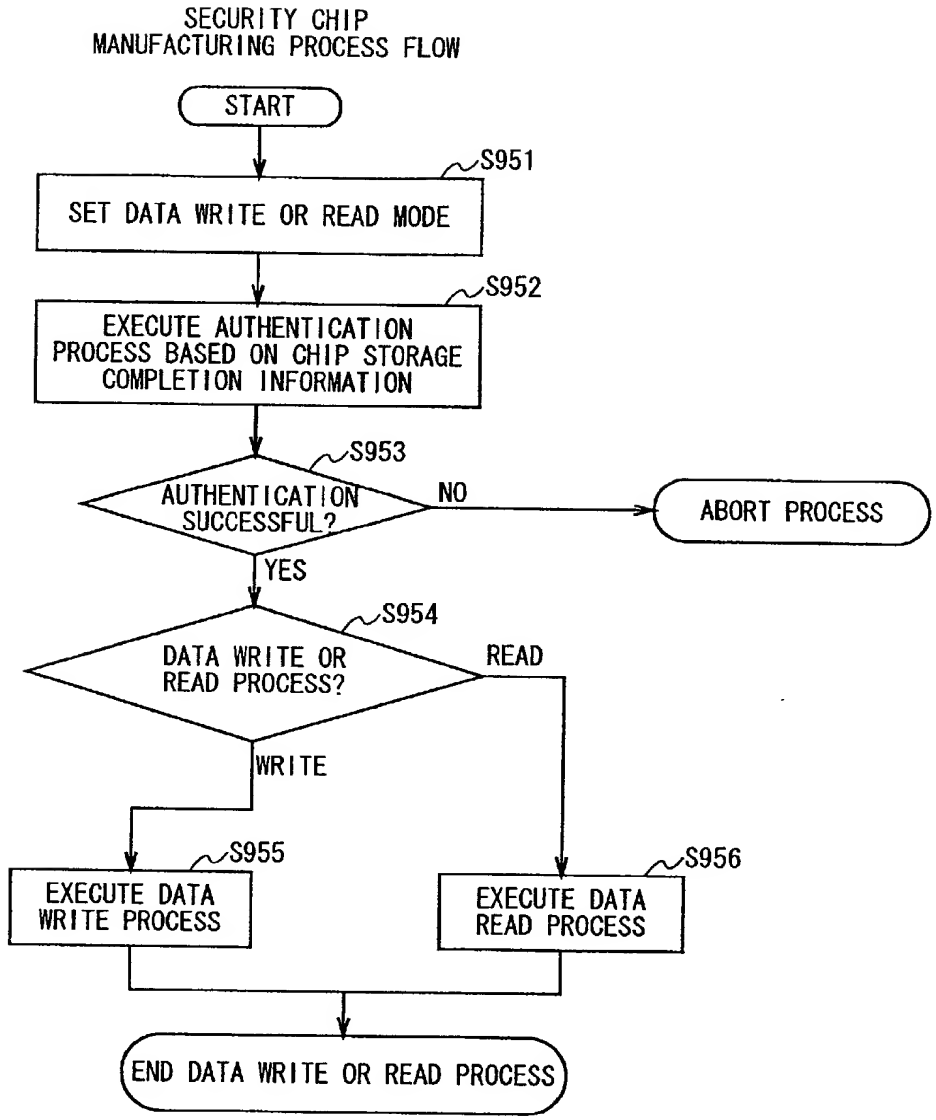
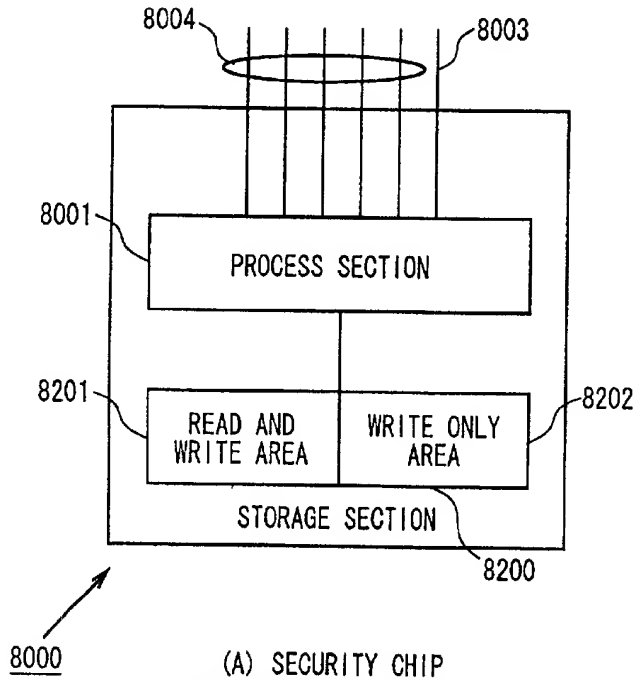
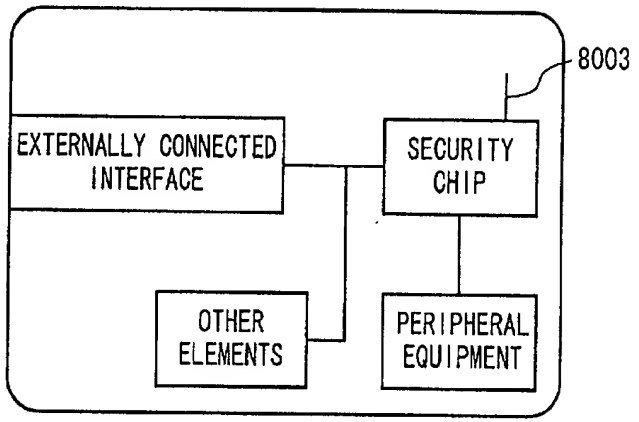

SECURITY CHIP
MANUFACTURING PROCESS FLOW
START
S951
SET DATA WRITE OR READ MODE
S952
EXECUTE AUTHENTICATION PROCESS BASED ON CHIP STORAGE COMPLETION INFORMATION
S953
AUTHENTICATION SUCCESSFUL?
NO
ABORT PROCESS
YES
S954
DATA WRITE OR READ PROCESS?
READ
WRITE
S955
EXECUTE DATA WRITE PROCESS
S956
EXECUTE DATA READ PROCESS
END DATA WRITE OR READ PROCESS

FIG. 90



(A) SECURITY CHIP
(MANUFACTURING PROCESS)



(B) PRODUCTS MOUNTED ON SECURITY CHIP
(EX. RECORDING AND REPRODUCING DEVICE AND RECORDING DEVICE)

FIG. 91

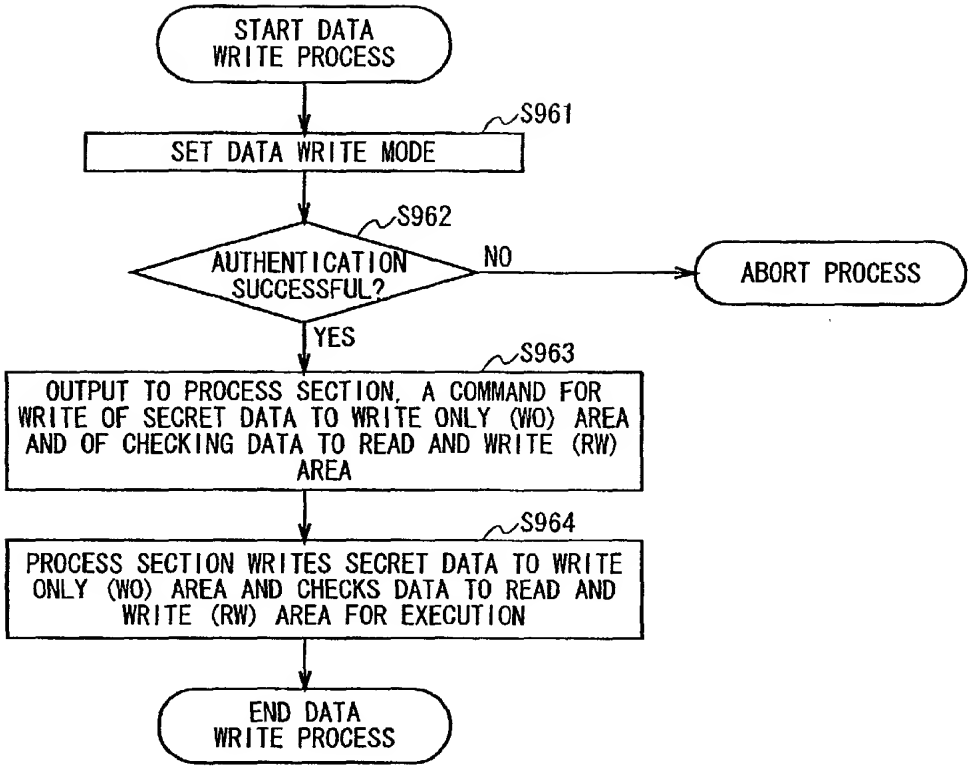

START DATA WRITE PROCESS
S961
SET DATA WRITE MODE
S962
AUTHENTICATION SUCCESSFUL?
NO
ABORT PROCESS
YES
S963
OUTPUT TO PROCESS SECTION, A COMMAND FOR WRITE OF SECRET DATA TO WRITE ONLY (WO) AREA AND OF CHECKING DATA TO READ AND WRITE (RW) AREA
S964
PROCESS SECTION WRITES SECRET DATA TO WRITE ONLY (WO) AREA AND CHECKS DATA TO READ AND WRITE (RW) AREA FOR EXECUTION
END DATA WRITE PROCESS

FIG. 92

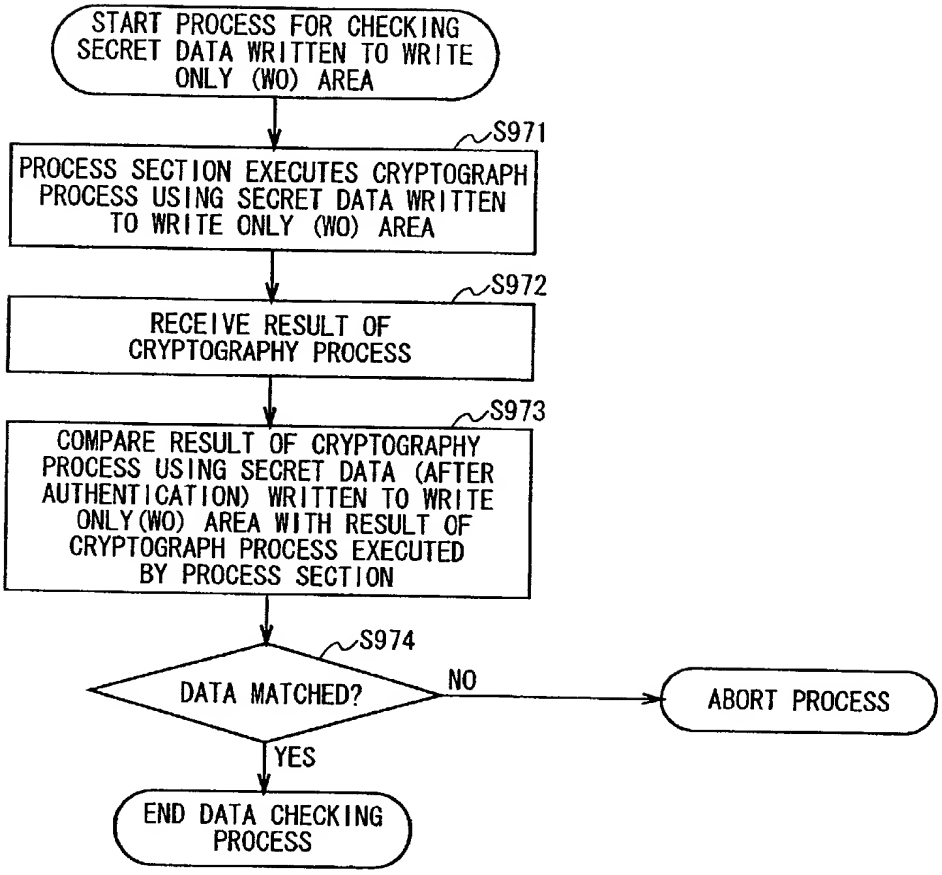

START PROCESS FOR CHECKING SECRET DATA WRITTEN TO WRITE ONLY (WO) AREA
S971
PROCESS SECTION EXECUTES CRYPTOGRAPH PROCESS USING SECRET DATA WRITTEN TO WRITE ONLY (WO) AREA
S972
RECEIVE RESULT OF CRYPTOGRAPHY PROCESS
S973
COMPARE RESULT OF CRYPTOGRAPHY PROCESS USING SECRET DATA (AFTER AUTHENTICATION) WRITTEN TO WRITE ONLY(WO) AREA WITH RESULT OF CRYPTOGRAPH PROCESS EXECUTED BY PROCESS SECTION
S974
DATA MATCHED?
NO
ABORT PROCESS
YES
END DATA CHECKING PROCESS

FIG. 93

Explanation of Reference Numerals

106...main CPU, 107...RAM, 108...ROM, 109...AV process section, 110...Input process section, 111...PIO, 112...SIO, 300...recording and reproducing device, 301...control section, 302...cryptography process section, 303...recording device controller, 304...read section, 305...communication section, 306...control section, 307...internal memory, 308...encryption/decryption section, 400...recording device, 401...cryptography process section, 402...external memory, 403...control section, 404...communication section, 405...internal memory, 406...encryption/decryption section, 407...external memory control section, 500...medium, 600...communication means, 2101, 2102, 2103...recording and reproducing device, 2104, 2105, 2106...recording device, 2901...command number managing section, 2902...command register, 2903, 2904...authentication flag, 3001...speaker, 3002...monitor, 3090...memory, 3091...content analysis section, 3092...data storage section, 3093...program storage section, 3094...compression decompression process section, 7701...content data, 7702...revocation list, 7703...list check value, 8000...security chip, 8001...process section, 8002...storage section, 8003...mode signal line, 8004...command signal line, 8201...read write area, 8202...write only area.